Long-Term Pavement Performance

Information Management System:

Operations Manual, VR 2.17

Publication No. TBD ?? 2015

US Department of Transportation
Federal Highway Administration

Research, Development and Technology
Turner-Fairbank Highway Research Center
6300 Georgetown Pike
McLean, Virginia 22101-2296

FOREWORD

The FHWA Office of Infrastructure R&D conducts and oversees research and development programs and projects that address critical highway infrastructure needs and priorities of national importance. Studies focus on the design, materials, construction, operation, and preservation of highway pavements, bridges, culverts, tunnels, and other structures. In addition, the Office of Infrastructure R&D provides expert technical assistance to other FHWA offices, other Federal agencies, State and local transportation organizations, industry and academia.

This document describes the processes used to manage the LTPP Information Management System (IMS) and its component hardware and software.

Jorge Pagán-Ortiz
Director, Office of Infrastructure
Research and Development

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No. TBD	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle LONG-TERM PAVEMENT PERFORMANCE INFORMATION MANAGEMENT SYSTEM OPERATIONS MANUAL		5. Report Date May 2010 6. Performing Organization Code
7. Author(s) Miriam Pitz and Tommy Clark, revised Barbara Ostrom		8. Performing Organization Report No.
9. Performing Organization Name and Address Scientific Applications International Corporation (SAIC) 151 Lafayette Dr., Oak Ridge, TN 37830		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH61-09-F-00046
12. Sponsoring Agency Name and Address Office of Infrastructure Research and Development Federal Highway Administration 6300 Georgetown Pike McLean, VA 22101-2296		13. Type of Report and Period Covered Operations Manual, May 2009 – May 2010, rev May 2010-November 2012, November 2013 14. Sponsoring Agency Code
15. Supplementary Note Contracting Officer's Representative (COR): Yan (Jane) Jiang, HRDI-30		
16. Abstract This document provides information about the Long-Term Pavement Performance (LTPP) Program's database operations. This document provides specific information about maintaining and upgrading the LTPP database servers, operating systems and software, performing DBA functions, tracking change requests, and producing the annual Standard Data Release. It provides information about using the LDEP Application, including running QC programs, data loaders and entering data into the Pavement Performance Database (PPDB) with data entry forms. References to the Traffic Analysis Software (LTAS) are included. In addition, it provides an overview of regional activities that relate to the database and data entry applications.		
17. Key Words Database, database server, general pavement studies, LTPP, pavement performance, specific pavement studies, LTAS, operating system, LDEP, AIMS, central database, server maintenance, anti-virus, backup software, relational database, database tools, SDR, standard data release, DBA functions, user administration, SPR, software release, QC output, data loaders, data entry forms, QC Manual.	18. Distribution Statement	

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 131	22. Price

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

PREFACE

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
		AREA		
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
		VOLUME		
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
		NOTE: volumes greater than 1000 L shall be shown in m^3		
		MASS		
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
		TEMPERATURE (exact degrees)		
^oF	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	^oC
		ILLUMINATION		
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	$candela/m^2$	cd/m^2
		FORCE and PRESSURE or STRESS		
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
		AREA		
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
		VOLUME		
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
		MASS		
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
		TEMPERATURE (exact degrees)		
^oC	Celsius	1.8C+32	Fahrenheit	^oF
		ILLUMINATION		
lx	lux	0.0929	foot-candles	fc
cd/m^2	$candela/m^2$	0.2919	foot-Lamberts	fl
		FORCE and PRESSURE or STRESS		
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380.
(Revised March 2003)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

Acronym		Definition
ADEP	–	AIMS Data Entry Portal
AIMS	–	Auxiliary Information Management System
CN	-	construction number
CPU	-	critical patch update
CSSC	–	Customer Support Services Contractor
CTDB	-	Central Traffic Database
DPW	–	Data Processing Workstation
FHWA	-	Federal Highway Administration
GB	-	gigabyte
IMS	-	information management system
KB	-	kilobyte
LDEP	-	LTPP data entry portal
LTAS	–	LTPP Traffic Analysis Software
LTO	-	Linear Tape Open
LTPP	-	Long-Term Pavement Performance
MB	-	megabyte
PDE	-	Public data extraction
PPDB	–	Pavement Performance Database
SAS	-	serial attached SCSI
SATA	-	serial ATA
SDR	-	standard data release
SPR	-	software performance report
TB	-	terabyte
TFHRC	-	Turner-Fairbank Highway Research Center
TSSC	-	Technical Support Services Contract
TSSC	–	Technical Support Services Contractor
UPS	-	Uninterruptible Power Supply
VA	-	volt amp

INTRODUCTION

This manual is intended to support server and database operations for the LTPP Information Management System (IMS). The LTPP server is located at Turner-Fairbank Research Center (TFHRC). It is referred to in this document as the central server. Other machines also under the control of FHWA's LTPP team are also addressed.

The LTPP IMS includes the Pavement Performance Database (PPDB), tables for the LTPP Traffic Analysis Software (LTAS), and the Ancillary Information Management System (AIMS). Applications that may be run on the central server will be discussed in this manual either explicitly or by reference to other documents identified in Appendix T. Reference Documents. Some of these programs were utilities written to accomplish a task and were not intended for general distribution. However, the majority of the programs are part of the LTPP data entry portal (LDEP), AIMS data entry portal (ADEP) or LTAS applications.

Information for each principal computer provided by FHWA including hardware, warranties, maintenance activities and software is included.

A limited discussion of regional operations is provided. The discussion is not intended to be an exhaustive list of regional activities, merely an overview of the elements that affect IMS operations.

LTPP SYSTEM OVERVIEW

LTPP PROGRAM

The LTPP program was established as part of the Strategic Highway Research Program (SHRP) in 1987 and has been managed by the Federal Highway Administration (FHWA) since 1992. LTPP was designed as a partnership with the States and Canadian Provinces.

The LTPP program is an on-going study of the performance of in-service pavement sections across the United States and Canada. These pavement sections have been constructed using highway agency specifications and contractors and have been subjected to real-life traffic loading. Pavement sections that are part of the LTPP program are categorized as General Pavement Studies (GPS) and/or Specific Pavement Studies (SPS). GPS consist of a series of studies on nearly 800 in-service pavement test sections throughout North America. SPS are intensive studies of specific variables involving new construction, maintenance treatments, and rehabilitation activities. Refer to the QC Manual, listed in Appendix T. Reference Documents for a list of GPS and SPS experiments.

LTPP DATA

The majority of LTPP data has been collected by four Regional Support Contractors (RSCs). Each RSC is responsible for data collection in a region of North America. The RSCs coordinate with state and provincial highway agencies (SHAs) in their regions to collect many types of data including details of maintenance and rehabilitation activities, coring and sampling activities, collection of site-specific weather data, drainage and traffic data. RSCs also collect deflection (FWD), distress, friction, longitudinal profile and transverse profile data. Regional date entry and validation are conducted using the LTPP Data Entry Portal (LDEP) and AIMS Data Entry Portal (ADEP) web-enabled systems linked to the production instance.

LTPP Information Management System (IMS)

The LTPP IMS is comprised of all the information collected as part of the LTPP Program. This includes electronic data and data on paper datasheets, in addition to documents, raw data files, videos, meeting minutes, software, reports, products, and much more that is not easily captured in a relational database. The two major IMS components are the Pavement Performance Database (PPDB), and the Ancillary Information Management System (AIMS).

The electronic data and data collected using paper forms are loaded, processed, and stored in the Pavement Performance Database (PPDB). The electronic files, paper data forms and other types of LTPP information are considered part of the ancillary information management system (AIMS) (figure 1).

The PPDB is a relational database that contains data elements that are easily organized into relational tables. Included in the same database instance are the tables used by the LTPP Traffic Analysis Software (LTAS) to generate information for the PPDB's traffic module.

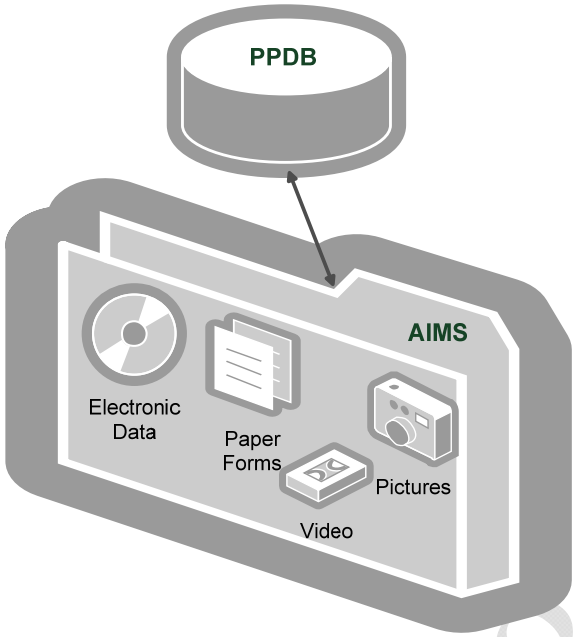


Figure 1. Schematic. LTPP Information Management System (IMS).

There are multiple copies of the PPDB and AIMS associated with different functions of the IMS.

Central Database

The LTPP database and AIMS are maintained at Turner-Fairbank Highway Research Center (TFHRC) as part of the Technical Support Services Contract (TSSC). This database serves as the record or archival copy. It may be referred to in some documents as a data repository.

The data in the central database is updated quarterly from the production instance. The AIMS files are updated annually and on the completion of regional contracts. Data provided by outside contractors and not through the RSCs is typically loaded by the TSSC to the LDEP rather than directly to the central server.

LTPP Data Entry Portal

A database production instance is maintained off-site for data entry by all LTPP contractors. Modifications to the database using development and test instances are also off-site but also accessible to LTPP regional contractors via the web. The server used is referred to as the Data Processing Workstation (DPW).

The LTPP Data Entry Portal (LDEP) application includes data entry forms, data loaders, Quality Checks (QC) programs and utilities (see figure 2). This application is the user's interface with the regional data. The user can enter, review, edit and delete data from the database with this application. Data entry and revision to tables not supported by forms or loaders is done via SQL scripts.

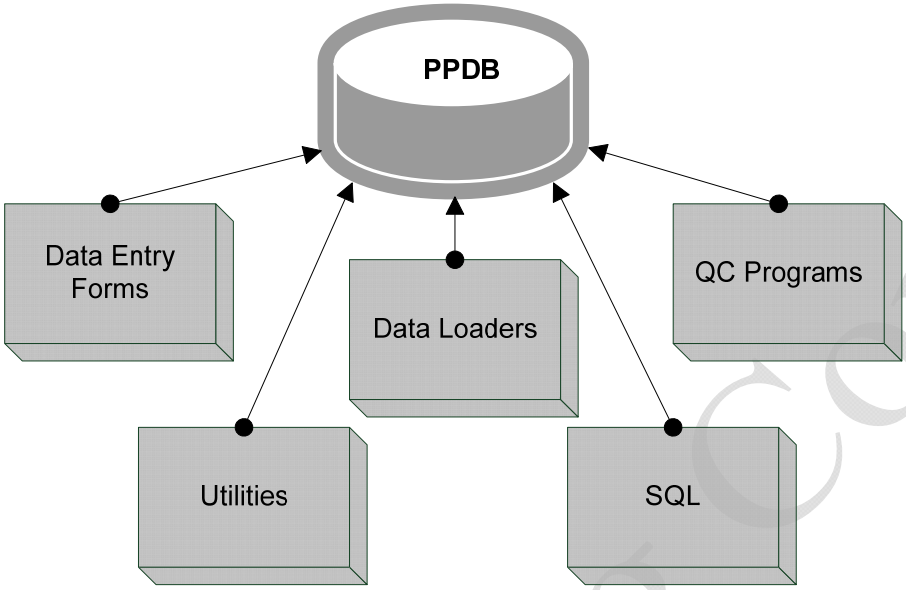


Figure 2. Schematic. LDEP Application provides access to PPDB.

AIMS Data Entry Portal

The AIMS Data Entry Portal (ADEP) application is a directory structure on the DPW to store AIMS data by region in a Subversion environment. The user can add, move and delete data from AIMS using Tortoise SVN.

LTPP Traffic Analysis Software

The LTAS application uses a set of tables within the PPDB. The outputs of the software support data and computed parameters tables in the PPDB. Prior to the implementation of LTAS version 2.0 the tables were stored separately from the PPDB.

The LTAS application is the user's interface to the traffic analysis tables. The raw hourly and vehicle traffic data goes through automated checks as it is loaded and summarized to daily data records. Then, the daily records go through another series of automated checks and are summarized to monthly records. Finally, the monthly records are checked and summarized to annual records. The LTAS application provides tools to analyze the data including running the QC process, purging data, graphing data sets and reporting.

The LTAS Application is documented in the following volumes of the LTPP Traffic Software Materials Reference:

- Volume 1 – LTAS Users' Guide
- Volume 2 – LTAS Graphics Specifications
- Volume 3 – LTAS Oracle Table Specifications, Codes and QC
- Volume 4 – LTAS Functional Specifications
- Volume 5 – LTAS Program Design Specifications

More information on LTAS documentation is included Appendix T. Reference Documents.

Pavement Performance Database

The Pavement Performance Database (PPDB) is an Oracle database structured for efficient data storage that contains many types of pavement performance data including materials testing, monitoring, maintenance and rehabilitation. It also includes the tables for the LTAS application.

Production Instance

The production instance is used for data entry, validation and computations for LTAS. Each region entering data has access only to the data for that region. The TSSC and Customer Support Services (CSSC) have access to all data for validation and rights to enter data collected or computed by others. Data validation by the TSSC is done on a periodic basis with all active modules checked at least annually.

In the fall of 2009, the archival copy of the production instance moved to the Federal Highway Administration (FHWA) Headquarters at the Turner-Fairbanks Highway Research Center (TFHRC) in McLean, VA. It is housed on a Dell R515 server with attached storage using Windows 2008R2 Server and an Oracle 12c database.

Development/Test Instances

Both a development database instance (IMSDev) and a test database instance (IMSTest) are included with the LDEP. These instances, or versions, of the database are used to develop and test updates to the production system. They are accessible to all users to test data entry via scripts. Validated updates and data changes are subsequently applied to the production instance.

A development database instance (IMSDev) and a test database instance (IMSTest) are also housed with the production database at TFHRC in McLean. These instances of the database are used for local testing and development. They are not synchronized with the LDEP instances of the same name.

PPDB Data Modules

The PPDB contains approximately 15,000 data elements that are organized into more than 600 tables. These tables are grouped into data modules by data type. For example, the Rehabilitation Module contains 54 tables that contain data about various rehabilitation events that have taken place on each section. Table 1 lists the modules and submodules that comprise the PPDB. With the exception of the tables in the Administration module, the first three letters of the table name (Table Prefix) identify the module to which a particular table belongs. Tables resulting from data compilation views are excluded. Tables used by the LTAS application are not included. For more detailed information about each module and the data it contains, refer to the *Long-Term Pavement Performance Information Management System User Guide* (IMS User's Guide) listed in Appendix T. Reference Documents.

Table 1. PPDB Data modules and submodules.

Data Module	Table Prefix	Description
Administration	None	This module contains tables that describe the structure of the database (LTPPDD, LTPPTD) and coded values used (CODES, CODETYPES, REGIONS). It also contains the master test section control table (EXPERIMENT_SECTION), the section location table (SECTION_COORDINATES), the section layering table (SECTION_LAYER_STRUCTURE), a regional lookup table (REGIONS), and a table of general section comments (COMMENTS_GENERAL).
Automated Weather Station	AWS	This module contains data collected by the LTPP program from automated weather stations installed on some SPS projects.
Climate	CLM	This module contains data collected from offsite weather stations that are used to compute a simulated virtual weather station for LTPP test sections or project sites. Data in this module are updated at 5-year intervals and was last updated in 2013 with data through 2012.
	MERRA	This module contains data based on Modern-Era Retrospective Analysis for Research and Applications (MERRA), a model developed by the National Aeronautics and Space Administration.

Data Module	Table Prefix	Description
Dynamic Load Response	DLR	This module contains dynamic load response instrumentation data from SPS test sections located in North Carolina and Ohio.
Ground Penetrating Radar	GPR	This module contains Ground Penetrating Radar (GPR) measurements performed on a subset of LTPP sections which provide an estimate of layer thickness variations within the monitoring portion of the test section.
Inventory	INV	This module contains inventory information for all GPS test sections and for SPS sections originally classified in maintenance and rehabilitation experiments.
Maintenance	MNT	This module contains information on maintenance-type treatments reported by a highway agency that were applied to a test section.
Monitoring	MON	This module contains pavement performance monitoring data and it is the largest module in the database. It is divided into submodules by data type:
Deflection	MON_DEFL	This submodule contains data from FWD tests.
	BAKCAL	This submodule contains backcalculation results from deflection data available through January 2013.
Distress	MON_DIS	This submodule contains distress survey data from both manual and film-based (PADIAS) surveys.
Drainage	MON_DRAIN	This submodule contains information on the inspection of drainage features.
Friction	MON_FRICTION	This submodule contains friction measurements taken by participating highway agencies.
Profile	MON_HSS	This submodule contains longitudinal profile data collected by an automated profiler or by manual dipstick measurements. Beginning with SDR 29 texture measurements are also included.

Data Module	Table Prefix	Description
Rut	MON_RUT	This submodule contains rutting data measured using a 1.2-m (4-ft) straightedge. These data tables are superseded by the rutting indices located within the Transverse Profile module. (Note: Straightedge rut measurements were not taken on all test sections.)
Transverse Profile	MON_T_PROF	This submodule contains transverse profile data and computed transverse profile distortion indices (rut depth) from manual dipstick measurements or the optical Pavement Distress Analysis System (PADIAS) method. Cross slope data is included in this submodule.
Rehabilitation	RHB	This module contains information on rehabilitation treatments.
Seasonal Monitoring Program	SMP	This module contains SMP-specific data, such as the onsite air temperature and precipitation data, subsurface temperature and moisture content data, and frost-related measurements.
Specific Pavement Studies	SPS	This module contains SPS-specific general and construction information for the SPS-1 through -9 experiments.
Traffic	TRF	This module contains traffic load, classification, and volume data.
Test	TST	This module contains field and laboratory materials testing data. A key table in this module is TST_L05B, which contains layer thickness and composition information based on measurements from the test section site.

Ancillary Information Management System

The AIMS is a collection of information not contained in the PPDB, such as raw profile and deflection data, distress photographs and images, reference documents, experiment guidelines, test protocols, LTAS output files, etc.

LTPP began to catalogue and archive data (using the AIMS metadata) with the intent to provide the public with information about the availability of the AIMS online so that they may request this data through the LTPP Customer Support Services Center. A majority of the AIMS data is available through InfoPave™.

AIMS items combined with the PPDB database are vital to the program's mission because they represent the LTPP legacy.

HARDWARE

The LTPP Program has provided servers and workstations to key contracts at various points over the life of the program. Currently the only program provided hardware is the servers at TFHRC and the DPW. This version of the document addresses four systems. They are the central server, the old central server, the DPW, and the workstation.

The central server is located at TFHRC and is the archival server for the LTPP program. Any references to TFHRC server, central server, the software, hardware or related activities are associated with the server that was purchased and installed at TFHRC in 2014. It may also be referenced as the Dell R515 or Dell PowerEdge™ R515, its model name, 10.10.10.34, its IP address on the internal TFHRC I2 network, or 192.168.2.26, its address on the LTPP network. Documentation on it is contained in the main body of this document and in various single alpha labeled appendices, i.e. Appendix A. Roles and Responsibilities – TFHRC Server.

Any references to the old TFHRC server refer to the server purchased in 2009 intended to be the original central server and archival location for LTPP data. It may also be referenced as the Dell 2900 or Dell PowerEdge™ 2900 which reflects the model name, I2-LTPP its name on the internal TFHRC I2 network, 10.10.10.29, its IP address on the internal TFHRC I2 network or 198.162.2.25, its address on the LTPP internal network. This server is not connected to the I2 network without prior notification to the TFHRC Help Desk. Documentation specific to this server which is still operation is found in appendices with an Aa labeled appendix, i.e. Appendix AC. Disaster Recovery – Dell 2900.

The Data Processing Workstation (DPW) is a server maintained off-site for production work. It contains the working version of the database for use by LTPP's regional contractors. This document contains limited information on the hardware and software elements of that system. It only addresses the current hardware installed in 2014. Information on the system installed in 2009 included in earlier versions of this document has been removed. The old system is inactive and retained off-site for disaster recovery purposes. This document does contain the security information, continuity and disaster recovery documentation for the DPW. The information on hardware maintenance and troubleshooting is the same as for the central server.

Central Server (TFHRC)

The central server was purchased in September 2013 and is located at FHWA headquarters at TFHRC in McLean, VA. It is a Dell PowerEdge™ R515 running Windows Server 2008 R2 Standard, SP 1. Two Dell PowerVault™ MD1200 storage units are attached. The central server was purchased with the vision to be a central repository located at a FHWA facility instead of contractor facilities.

The server is also designed to be somewhat fault tolerant. It features multiple power supplies and hot swappable hard drives. While the uptime requirements of the LTPP server are not that high, this redundancy helps to keep the systems running while waiting

on parts to arrive. On the down side, without someone checking the system for faults on a regular basis, the servers can keep running for a long time with failed parts. This can lead to a loss of data if, for example, one hard drive has already failed and another fails before the first failure is repaired.

The hard drives on the Dell R515 are joined together in a single RAID 1 array. They are associated with the PERC 7000. The attached storage units controlled by a PERC H800 control as RAID-6 with 2 arrays of 32 TB capacity each. The hard drives are partitioned into volumes and these volumes are set aside for different purposes. Microsoft Windows Server is installed on the C: volume. *The Oracle database files are stored on the D: volume.*

The server was delivered with the Windows Server 2008 R2 Operating System. This was then configured to comply with NIST 800-53 Revision 2 Annex 1 since this is a low impact system. When setting up the server various utilities such as the backup software were installed. Then the Oracle database software was installed and the database instances created.

This server is run on an internal I2 TFHRC network and is not a domain controller. It has two network controller cards. The second is attached to a… switch for use on an internal LTPP network with three devices, the central server, the Dell 2900 and a personal computer. Server maintenance and troubleshooting is discussed in Appendix D. Hardware Maintenance.

Operating system updates are acquired automatically and applied manually on notification of availability. Anti-virus updates are done automatically. Oracle updates and patches are done on an as needed basis. The upgrade from Oracle 11g to Oracle 12c was done in summer 2014.

The system has a 64-bit version of Oracle 12c with 32-bit Oracle 11g and 12c clients to run LTPP specific software. Instances in the Oracle installation include IMSProd, IMSTest, IMSDev and SDR29. The SDR29 instance is a static copy of the information provided for public distribution via InfoPave™.

Data Processing Workstation (DPW)

The Data Processing Workstation is the development machine for updating PPDB data as well as the development environment for IMS and Traffic Analysis software. It is a Dell PowerEdge™ R515 purchased in 2013 as a replacement for a Dell PowerEdge™ 2900 server. The DPW is located off-site. It has two Dell PowerVault™ MD1200 storage units.

The Dell 2900 is available as a failover machine. It has two 1.86 GHz Xenon 5150 dual-core processors. It also has 2 GB of RAM and a RAID 5 array consisting of seven 10,000 RPM 146 GB SAS disks. For backups, it has a PowerVault RD1000 which accepts 1-TB hard disk cartridges. All of this is protected by a 2200 VA UPS.

The Dell R515 was received with Windows 2008 R2 installed. As a test of recovery procedures the OS was removed and a bare metal recovery done of the OS and the applications on the Dell 2900. Following a successful recovery, all existing applications and data were transferred to the new server. The two systems were operated in parallel for a month to verify that all applications were working correctly.

Backups

The original central server and DPW use Symantec Backup Exec and RD1000 500GB and RD1000 1TB Disk cartridges for backups. The replacement units use 4 TB hard drives for large backups, both annual submissions and AIMS.

While the backup software (versions) and devices vary, both machines use a similar backup strategy. That is regular backups of the Oracle database to removable media. Due to the fact that most information entered into the database comes on either paper forms or electronic data sets, the risk of data loss is low. Therefore, a bi-weekly backup to removable media has been chosen as the proper balance between risk and cost for the central server. A weekly backup to removable media is done for the DPW since the data and software are until continual revision. Incremental backup policies vary by location. Due to the less frequent updating of the central server, incremental backups are performed on alternate days rather than daily.

SOFTWARE

LTPP uses a combination of off-the shelf and custom software. Both systems use Windows Server 2008, SP 2 on the Dell R515s. The DPW software includes Redmine, Apache Tomcat and other packages not used on the central server.

The following is a list of key software packages that are loaded on the LTPP machines to facilitate operations.

- Windows Server 2008 - Operating system patches are applied through Windows update on a monthly basis. The process is set for manual rather than automatic updates even though the computer is typically on and connected to the Internet. Updates are also applied as requested by the TFHRC Help Desk.

- Symantec Anti-Virus - *Symantec Endpoint Protection 11.0.2000.1567 is* being used on the central server. This is the FHWA required antivirus program. *It requires a manual update to ensure all elements are current.*

  Symantec Anti-Virus is being run on the DPW.

- Symantec Backup Exec 2010 - Symantec Backup Exec 2010 is being used to perform backups to RD1000 disk cartridges. It requires manual updates to remain current. The product on the Dell Poweredge 2900 was supported through February 2014.

- *Symantec Backup Exec 2015 – Upgrade from Symantec Backup Exec 2014 for the central server.*

- Oracle - Oracle was chosen early in the development of the IMS. At the time, it was one of the only tools which could handle large databases across multiple hardware platforms. Oracle also had a forms and reports package for application development which was able to run on multiple platforms without recoding.

  Oracle software updates have generally only been applied during major system upgrades. The DPW which houses a central repository is on an isolated network with access limited to LTPP personnel. The central server is on an isolated network with access limited to LTPP personnel as well.

  The Oracle Database Enterprise Edition version 11.2.0.1.0 along with the administrative tools is installed for use with the PPDB on the Dell 2900. *Add reference on location of documentation locally and on-line.*

  The Oracle Database Enterprise Edition version 12….. along with … is installed for use with the PPDB on the Dell R515. *Add reference on location of documentation locally and on-line.*

- APEX - This is an Oracle provided web-based SQL application that is used on the DPW. It provides the ability to run SQL scripts and get limited types of output. Scripts may be edited, uploaded and stored in the application.

- SQL Developer - SQL Developer is a GUI provided by Oracle that allows manipulation of both data and the databases. This software replaces the use of Enterprise Manager on the TFHRC server. Limited documentation on the more common LTPP uses of this tool is found in Appendix M. SQL Developer Notes.

- Enterprise Manager - This is Oracle software that provides a Graphical User Interface (GUI) with which to view and manage database objects (tables, views, indices, tablespaces, users, etc.). This software is installed on the server when the Oracle RDBMS is installed and is installed on the workstation when the Oracle Client is installed. This tool is no longer commonly used. This software has been removed and replaced with Oracle SQL Developer.

- SQLPlus Worksheet - The SQLPlus Worksheet is an Oracle client tool that allows the user to type SQL*Plus commands in an input window and see results in an output window. Commands are executed by pressing F5 or CTRL-Enter. Previous commands can be accessed by pressing CTRL-p and next commands by pressing CTRL-n. Other shortcuts are available in this tool. This tool has been replaced by SQL Developer and Apex in daily use.

- Command Prompt - SQLPlus and Oracle utilities can be executed from a Command window by users with permissions to access the server directly. For example, a sqlplus file (.sql) can be executed with the following syntax:

```
sqlplus connectstring @sqlfile.sql
```

The Oracle data export command can be executed as follows:

```
exp connectstring parameters.par
```

where the parameters.par file has all input parameters. The same list of parameters can be included on the command line.

Work on the central server has not migrated to Power Shell although it is available.

- PowerDesk (Central Server) - PowerDesk is file management software similar to Windows Explorer. Its advantage over Windows Explorer is that the results of directory searches may be save to text (.txt) or comma separated value (.csv) files. This product requires a license.

- Notepad++(Central Server) - This is a text editor. It is a free source code editor distributed under the GPL license. It is similar to Notepad or Wordpad. Its advantages are that it can do columnar cut and paste, it has basic syntax checking capabilities for SQL and other languages and files can be opened in more than one tool using a text editor and they will be synchronized. The last capability makes it possible edit scripts in Notepad++ and after saving them, run them in SQLDeveloper while having them open in both applications.

- Microsoft Office (Dell 2900) - Microsoft Office has been installed on this machine primarily to provide Microsoft Access for extracting tables for LTPP applications requiring tables in this format. It is possible to update this software using the same procedure outlined in the preceding Operating System Updates section. Just choose Microsoft Access as the product.

  Office has been installed in order to process data releases efficiently. Since data releases are provided in Microsoft Access format, it is very important to have Office tools available.

  The software is updated through the Windows Update function at the same time operating system updates are done.

  Software upgrades no longer require the actual installation of MS Office and it is not installed on the Del R515.

- Spiceworks (Central Server) - This is third party freeware for network management. The software was installed to generate a list of installed applications for IT Security documentation. None of the other functionality is used.

- Redmine (DPW) - Redmine is a project management web application. It is open source software distributed under the GNU General Public License v2. The

software is used for track issues with data and software and track action items and operational activities.

TRACKING PROCESSES

The DPW workstation contains the mechanisms to track data and programming issues with both the PPDB and LTAS and action items from various meetings. Access to the various tracking areas varies as do permissions to make entries and modifications to those entries.

Issues/Software Performance Reports (SPRs)

Software Performance Reports (SPRs) have been used to document questions about and issues with the PPDB and all of its components since the beginning of the LTPP program. In addition, SPRs have been used to document new development for the LTPP applications. SPRs can be submitted by regional or central users of the database system. SPRs are recorded in the Redmine application at http://portal.ltpp.org under the Issues/SPRs tab. Users log into both the web site and the Redmine application.

After selecting the Issues/SPRs tab and logging into Redmine the user selects a subproject in the LTPP Database System project. The options for SPRs are:

- Data Update via Scripts – modifications to data using SQL scripts when forms do not exist for table modifications
- LTAS – data or software issues for the LTAS application
- PPDB – QC programs, loaders, LDEP forms, data entry issues,

Directive I-155 or the most recent version of it discusses how SPR information is entered for the PPDB and LTAS and the priorities assigned.

Software Change Notice (SCN) Report

Deployment of software updates is documented in Redmine in lieu of the previous Software Change Notice report. The changes deployed can be found by filtering the records in Redmine.

Software Deployment (DPW)

Deployment of changes to the PPDB forms and utilities takes place on a monthly basis. Changes which are critical to continuous regional data entry operations may be deployed between the monthly updates.

Deployment of LTAS changes is done on an as needed basis. Major changes to functionality are deployed after regional testing but typically no more than twice a year.

Action Items

Most LTPP team meetings and many teleconferences result in action items for follow up. These items are tracked using Redmine under Issues/SPRs and the Operations project. The Action Items subproject contains the tracking mechanism for these items.

RECURRING SERVER ACTIVITIES

Recurring server activities consist of backups, off-site data storage, software updates and system security.

Bi-weekly backups of electronic databases consist of a full backup of working directories done on alternate Tuesdays. Incremental backups of the database instances and other folders are done during the week. Quarterly backups of AIMS folders are done the 1st Wednesday of February, May, August and November. The outline of the process is included in Appendix G. Backups – An Illustrated How To. Instructions on how to use and maintain various elements of the backup software are contained in appendices of this document.

The software currently used for backups is *Symantec Backup Exec 2015 for Windows Servers*. It is LTPP licensed software. *Updates must be manually identified on the software's website and manually transferred to the server as long as the system is not connected to the Internet. The process for updates is discussed in SYMANTEC ADMINISTRATION AND TROUBLESHOOTING.*

FHWA has contracted with First Federal for off-site storage and a monthly delivery and pickup of storage boxes for electronic media. Changes to the schedule must be done by the COR. Additional information on this activity is found in Appendix H. Off-site Backup Process.

Software updates are done on an informal schedule. No updates are done automatically. Microsoft software is updated monthly unless a critical update is flagged by the DOT Help Desk. Anti-virus software is updated at the same time as Microsoft software. Oracle updates are done when a critical patch addresses a major security flaw or an operational issue that is preventing efficient LTPP operations. All other software is checked quarterly for updates.

The software for security (firewall etc) is Symantec Endpoint Protection. It is FHWA licensed software. It is not possible to update this software without an Internet connection.

The systems used by the LTPP program are expected to be FISMA compliant. Elements of the security plans for both the central server and the DPW are included with this document. All users of the systems are required to take DOT IT security training annually or have their accounts locked. Access to either system is subject to approval by the COR of the TSSC contract.

Backups

Frequency: Specified by data type and hardware

Tasking: Task D Leader

References: Symantec Backup Exec Administrator's Guide (pdf available with software); copy saved in G:\Working_space\Backup\References on server

Filing: Task_D..\1_Database Operation\a_Operating the Database\0_Backup_procedures – schedule spreadsheet

Task_D..\1_Database Operation\a_Operating the Database\1_First_Federal_off-site – schedule database

Task_D..\1_Database Operation\a_Operating the Database\2_Symantec_software – used for notes, references, e-mails, and other administrative matters

On the server –

- G:\Backup\References
- G:\Backup\Backup_logs – pdf copies of the log files from all backups by type (incremental, weekly, monthly, periodic) and backup selection criteria
- C:\Program Files\Symantec\Backup Exec\IDR\Data (disaster recovery alternate path)

External Hard Drive:

- *M:\Backup\IDR – ISO image for data recovery; \Data .dr data recovery files*
- M:\Backup\IDR\IDR_dr - .dr data recovery files
- M:\Backup\IDR\IDR_iso - .ISO image for data recovery
- M:\files for incremental backups and the associated indices

Server backups are done with Symantec Backup Exec 2010 R2 (BE) as of April 1, 2011. Backups are done with zSymantec.User as the user name. This user has the privileges needed to create backups and restore files from backups if required.

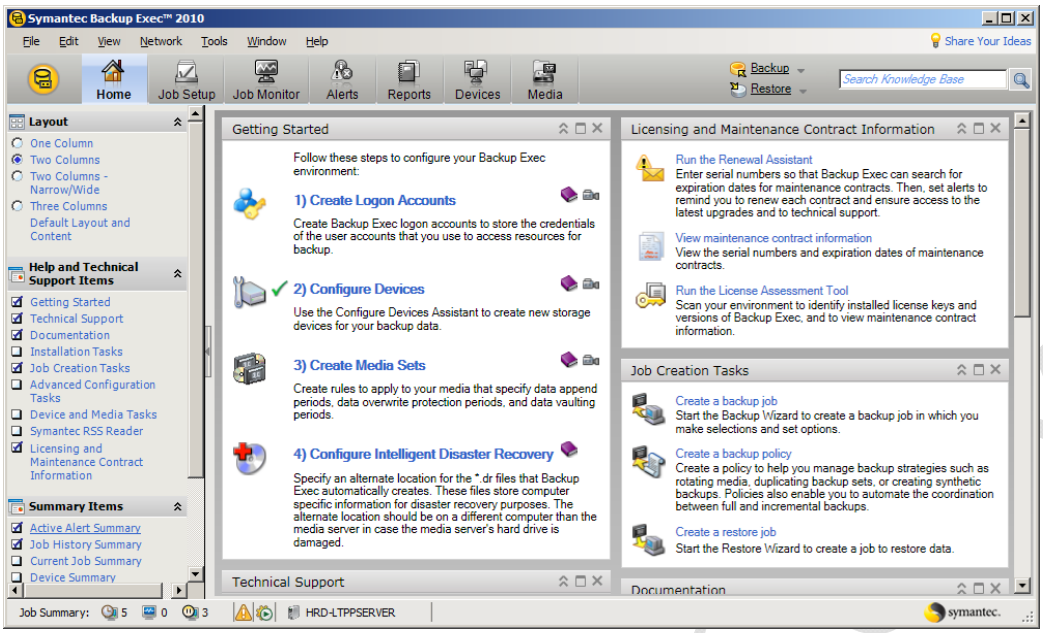


Figure 3. Screenshot. Home screen for Backup Exec 2010.

Cartridge backups are tracked using a spreadsheet which has the various schedules (offsite_rotationsvN.xlsx). *This file is maintained on the FHWA provided computer in the Task_D_IMS_Hardware-Software directory. The subfolder 0_Backup_procedures is located under a_Operating_the_database in 1_Database_Operation.*

The adopted backup schedule for the TFHRC server was derived from a document written by SAIC in July 2009 and implemented to reflect operations at TFHRC and the off-site storage schedule.

Full backups to removable media are done (excluding the contents of recycle bins):

Bi-weekly on Tuesday evenings for the C:\ and D:\ drives and selected folders on the F:\ and G:\ drives

Quarterly on the first Wednesday of February, May, August and November for AIMS material (K:\ excluding video), items of historical value and supplemental databases from outside sources.

Incremental backups to the external 2 TB drive (M:\) while the standard data release(SDR) is being prepared are done:

Three days a week (Monday, Wednesday, Thursday) for D:\ (LTPP Database), r F:\ (Traffic) and G:\ (Working Storage)

Incremental backups when the standard data release is not being processed:

1. Three days a week (Monday, Wednesday, Thursday) for D:\ (LTPP Database)

2. Two days a week (Monday, Thursday am) for F:\ (Traffic)

3. Two days a week (Wednesday, Sunday am) for G:\ (Working Storage)

The SDR processing period is defined to include the week prior to the receipt of data for the SDR through the week after the shipment of the SDR or other copy of the data to FHWA for permanent storage.

Work station backups are done as a part of G:\ drive backups using Windows backup capability to copy the material to a shared drive on the server.

Work Flow

The following lists the recurring activities associated with server backups. The number of incremental backups to be verified is the only thing that changes depending on whether a release is being processed:

Daily – verify that the scheduled backups have run

Bi-weekly – (Tuesday – prior to full backup)

Run preparation for disaster recovery (create .dr file - Preparing for Recovery)

Weekly – (Wednesday mornings) –

1. Verify the bi-weekly backup ran for odd Tuesdays in the quarter

2. Print (pdf) copies of all job logs and histories since the last weekly backup including incremental backups (in expanded format)

3. Move prior week's incremental pdfs to \Last_week folder

4. Erase weekly pdfs for the same tape name

5. Erase incremental backup pdfs more than 2 weeks old

6. Eject the current cartridge

7. Erase all job reports in Symantec BE after printing

8. Insert the tape to be used for the next backup, typically for the following bi-weekly backup

9. Inventory the cartridge and verify it has space for next backup

10. Erase folders on cartridge NOT created with BE if necessary (Windows Explorer)

11. Format a new cartridge if necessary

Fourth Wednesday of the month –Put cartridge for off-site storage in FFC container (or in desk drawer if container is off-site)

Quarterly

1. First Wednesday morning of second month –
2. Take AIMS backup job off hold
3. Verify selections for backup
4. Print a pdf of the backup conditions if modified
5. Print paper copy of the current AIMS backup properties for storage with the cartridges
6. Inventory 1TB cartridge to verify space available/overwrite conditions

First Thursday morning of second month (or Wednesday pm)

1. Put AIMS backup job on hold on completion
2. Print (pdf) copies of job log and history
3. Print a paper copy of the backup log for storage with the cartridges
4. Delete last pdf of backups to same cartridge(s)
5. Eject the current cartridge
6. Erase all job reports in Symantec BE after verifying pdfs exist
7. Insert cartridge for the next bi-weekly backup
8. Inventory the cartridge and verify it has space for next backup
9. Erase folders on cartridge NOT created with BE if necessary (Windows Explorer)
10. Format a new cartridge if necessary

Incremental Backups

Incremental backups are done using a folder on the 2TB external drive. Incremental backups are retained for two weeks before being overwritten. BE keeps track of the actual file retention.

Bi-weekly Backups

Since the ORACLE instances must be shut down prior to backup this may be done by including a pre-backup command script in the Symantec schedule and a post-backup command script to bring them backup up.

Quarterly Backups

Drives that only change with a release or a data transfer are backed up on a quarterly basis.

Off-site Storage

Frequency: Monthly (3rd Thursday) (established by COR)

Tasking: Task Leader - Task D

References: On-line Help for First Federal software

Filing: Task_D..\1_Database Operation\a_Operating the Database\1_First_Federal_off-site

FHWA LTPP has a contract with First Federal Corporation (FFC) to provide for off-site storage of electronic media. The contract is managed by the COR of the LTPP contract. All changes to the contract scope or activities must be done through and by the COR. Bi-weekly backups and quarterly backups are both stored off-site. The backup created prior to the most current one as of the pickup date is the one sent off-site. The most recent backup is retained on-site.

For Customer Service at First Federal Corp.: Mr. Matt Kough

301-548-9676 (Office)

301-963-8974 (Fax)

Email: Operations@ffederal.com

username: 700

password: FHA700

Badge ID: *** (the middle three letters of the user's FFC ID)

Setup date: 10/20/09

Work flow

A batch in FFC is a collection of boxes of the same type that will be sent to FFC. Returns are automatically generated based on the inventory information at FFC.

The second Friday of the month

Set up batch(es) with the box(es) to be sent to FFC that are at THFRC.

Verify that all the boxes that should be returned have return dates in Inventory for the third Thursday. Change the inventory if necessary.

The third Wednesday of the month send an e-mail to TFHRC Security to notify them of the courier's visit. The courier's name is not required, FFC (or First Federal Courier) is sufficient.

The third Thursday of the month

Add a batch if needed for a box that is being returned that day.

Mark up the box receipts with their label names to match against inventory after tape transfer

The third Friday of the month verify FFC inventory versus receipts.

Regular visits

Visits for return and pick up of media occur on the 3rd Thursday of every month except when that date is a holiday. The expected pickup time is between 9:30 and 11:30. Either TFHRC Security or the courier will call when the courier is on site. The courier is met at the front desk of the Turner building with any boxes being sent. A TFHRC individual with FFC identification must be present to log boxes in and out.

Setting up unscheduled visits

Unscheduled visits should only be required in the event of catastrophic failures (flood, fire, equipment failure) and inability to use current on-site backups to restore files. While the cost is not large, these visits must be cleared through the COR.

Obtaining First Federal credentials

The COR will contact First Federal with the necessary information to put the LTPP IMS DB Engineer on the list of approved FFC contacts to pick up and deliver media. An electronic ID (RFID) is provided. It is needed for confirmation of pickup and delivery as well as for access to the FHWA account on-line for scheduling.

HARDWARE CHECKS

The system is checked on weekdays to verify that no yellow/orange lights show on the front of any item. Any light that is not green (or blue) requires investigation. The steps to be taken are specific to the equipment and should be identified by using the relevant manual(s). *On a weekly basis the Dell Server Manager tool is used to check internal elements of the server and external storage including batteries, power supply and potential hard drive failures.* This check is generally done when the backup logs are saved.

All LTPP equipment is under warranty through either the LTPP program specifically or the FHWA IT unit. Repairs, if needed are to be coordinated with the COR. Only items that are hot swappable are "repaired" by the LTPP Database Engineer.

*Electronic copies of hardware manuals are located in …..*Hardcopy hardware manuals and CDs with users' manuals are kept in the right hand drawers of the desk with hutch in the server room. These should not be needed. The basic instructions on items to check before calling for maintenance are outlined in Appendices D. Hardware Maintenance and AD. Hardware, Software and Maintenance – Dell 2900.

The following manuals are present for the hardware:

Dell 2900 Server

MD Powervault storage

APC Smart UPS 2200, original unit

HP Procurve switch

REGIONAL OPERATIONS

Regional office operations are driven by the flow of data through the process shown in figure 4. All data entered into the LTPP Pavement Performance Database (PPDB), whether electronic or on paper forms, goes through the same basic process.

Data coming into a regional office is reviewed, often with the help of preprocessing software, and loaded into the database by filter or by entry form using the PPDB element of the LDEP. It is then checked by the Quality Checks (QC) software. Based on the results of the QC software, the data may go through a correction or upgrade process. Data is subsequently released to data analysts and researchers via InfoPave and the SDR. A more complete discussion of the process is included in the Long-Term Pavement Performance Data Entry Portal (LDEP) User Guide, November 2012. The steps in the process are:

1. Collect Data - Many resource documents exist to support data collection activities. Most collection activities are specified in directives from FHWA. For example, information on site selection, site preparation and data collection for AWS sites can be found in directive AWS-01.

2. Process Data - The type and format of the data determines how the data is processed. Some data is collected in electronic data files and some data is collected on a paper data sheet.

3. Data may be electronic or provided on paper forms.

    a. Electronic Data -Many data modules have at least some electronic data to process. Table 2 and Table 3 lists the data modules and the filter program(s) used with each module, as well as other module-specific information.

        i. Backup Raw Data - Raw data files should be copied to ensure that no data is lost in transit from field to office.

        ii. Review Data/Run Preprocessors - The header portion of electronic data files should be reviewed manually for required information. Automated preprocessing software checks much of the electronic data for correct format and reasonable values. For example FWD data is preprocessed with the FWDSCAN software; Longitudinal and Transverse Profile data is preprocessed with the PROQUAL software. This excludes the dipstick data.

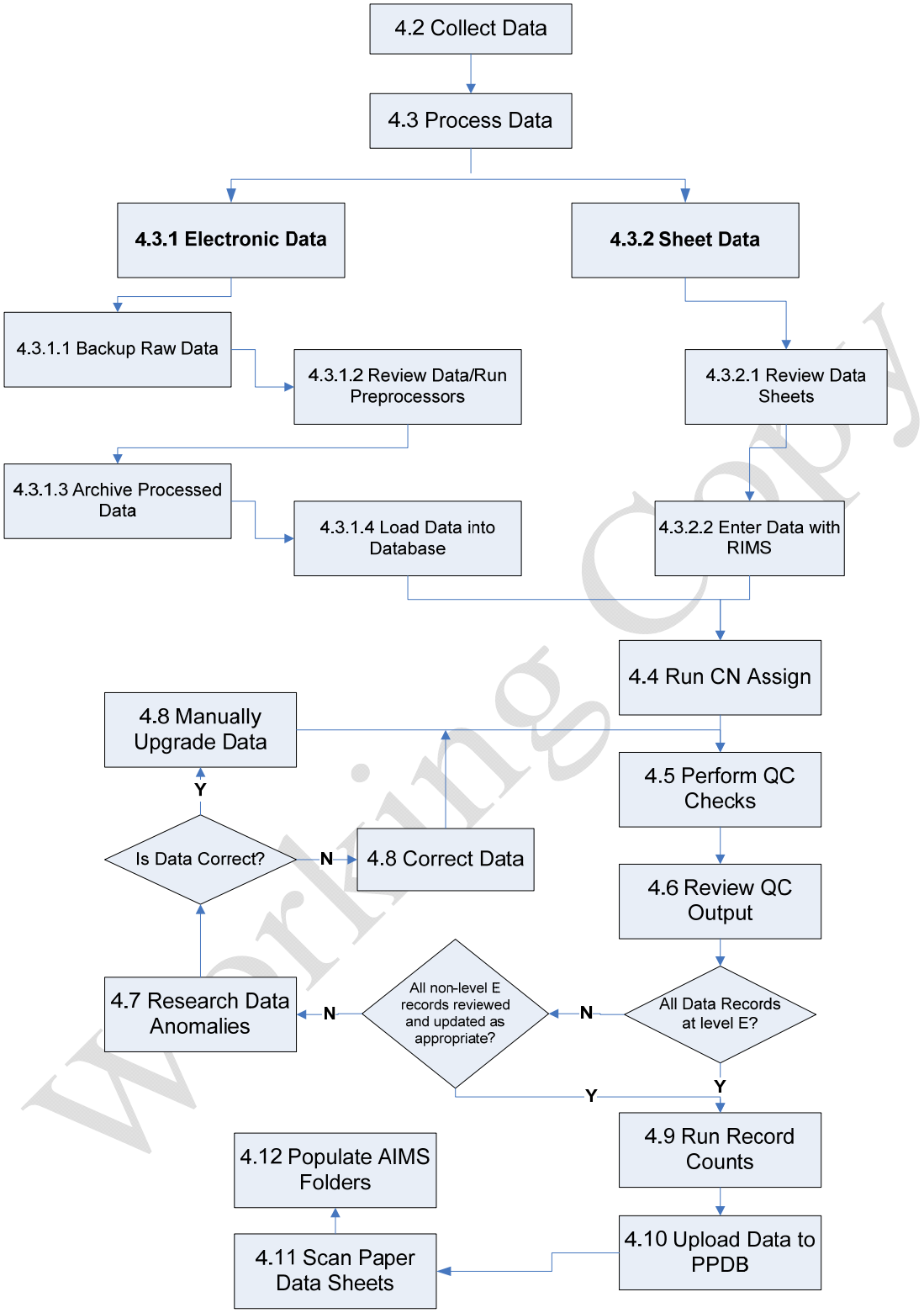


Figure 4. Flow Chart. Regional data flow diagram (replace).

Table 2. Filter, CN, and QC programs and chapters for active modules.

Data Module	Filter Program	CN	QC Program*	QC Manual Chapter
Administration	NA	N	EXP_QC AdminQC	Chapter 25
Auto Distress (Padias42)	CROSSSLOPELOAD PADIAS42		?? DISPAD42	Chapter 7
Climate	CLMLOAD	N	ClmOwsQC ClmVwsQC	Chapter 12
Deflection	FWD25LOD FWDCOMM PDDXLOAD		FWD25	Chapter 5
Friction	NA		FRICTION	Chapter 8
Maintenance	NA	Y	MNT_QC	Chapter 9
Manual Distress	JpccFault		DIS_QC	Chapter 7
Profile	PROFLOAD	Y	PROFQC	Chapter 4
Rehabilitation	NA	Y	RHB_*	Chapter 10
Test (Materials)	Aggshape MatActLoad MatLoad P46Load	Y	TST_* EstarQC P46 P07V2 PGBinderQC UnboundSpecGravQC	Chapter 3
Transverse Profile	TPRFLOAD CrossSlopeLoad TPRFCLOD		TPROF CrossSlopeQC	Chapter 6

* The asterisk in the QC program name indicates that there is a separate program for level C, level D, and level E QC (quality checks). For example, TST_* represents TST_C, TST_D, and TST_E programs.

Table 3. Filter, CN, and QC programs and chapters for inactive modules.

Data Module	Filter Program	CN	QC Program*	QC Manual Chapter
Auto Distress (Padias10)	PADIAS		DISPAD10	Chapter 7
Automated Weather Station	AWSLOAD	N	AWS	Chapter 23
Monitoring - Drainage	NA		MonDrainQC	Chapter 27
Dynamic Load Response	DLRLOAD_AC DLRLOAD_PCC	N	DLR	Chapter 24
Ground Penetrating Radar	GPRLOAD	Y	GprQC	Chapter 28

Data Module	Filter Program	CN	QC Program*	QC Manual Chapter
Inventory	NA	N	Init3 INV_QC	Chapter 2
Seasonal Monitoring Program	SMPLOAD TDRMANUALLOAD SMPFRAUT	Y	SMP_* TdrManualQC	Chapter 22
Specific Pavement Studies	NA	Y	SPS#_* SINIT#, # = 1,2,5,6,7,8 SPS_misc	Chs 13 – 21 and Chapter 26
Traffic	EST_TRAF TDSHEET4 TDSHEET5 TDSHEET7 TDSHEET8 TRFLOAD TRF_SPS	N	TRF_QC TrafficAnalysisQC	Chapter 11

* The asterisk in the QC program name indicates that there is a separate program for level C, level D, and level E QC (quality checks). For example, TST_* represents TST_C, TST_D, and TST_E programs. Some SPS# programs have additional divisions such as D1 and D2 or BC instead of just C.

iii. Archive Processed Data - Instructions for data archival can be found in the directives. In most cases, both processed data and raw data should be archived.

iv. Filter Data into Database - Table 2 and table 3 list the filter programs used for each module. The PPDB application includes forms from which each filter can be executed. An example is shown in Figure 5. The outcome of the processing can be reviewed by identifying the job from a list of background jobs from the left hand of the PPDB screen as shown in Figure 6.

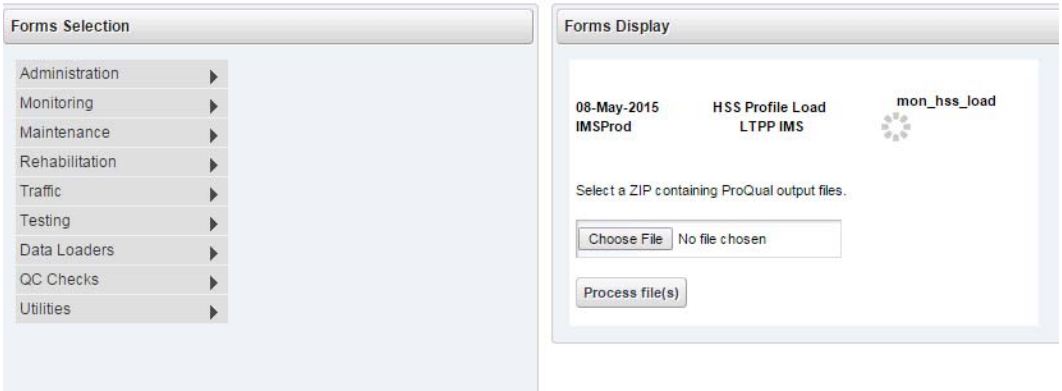


Figure 5. Screenshot. Example of data filter in PPDB.

Figure 6. Screenshot. Selecting a job to check.

b. Paper Sheet Data - Most modules have some sheet data to enter into the database. The exceptions are the CLM, DLR and Longitudinal and Transverse Profile data modules. Sheet data comes in the form of paper data sheets that may have been filled out by one of the state or provincial agencies or by a regional contractor on-site during construction or rehabilitation of an LTPP section. Some data modules are composed entirely of sheet data (INV, TST) and others have mostly electronic data with only one or two sheets of supporting information (FWD).

   i. Review Data Sheets - An engineer familiar with the LTPP section should review all data sheets submitted by an agency before the data is entered into the database. Questionable values or blank items should be researched and corrected.

   ii. Enter Data with PPDB Forms - *Basic forms instructions are included in the LDEP User's Guide. For specific information about each data entry form, refer to the Forms Index in the User's Guides section of the LTPP Operations Center.* Forms are grouped by module and in some cases by submodule.

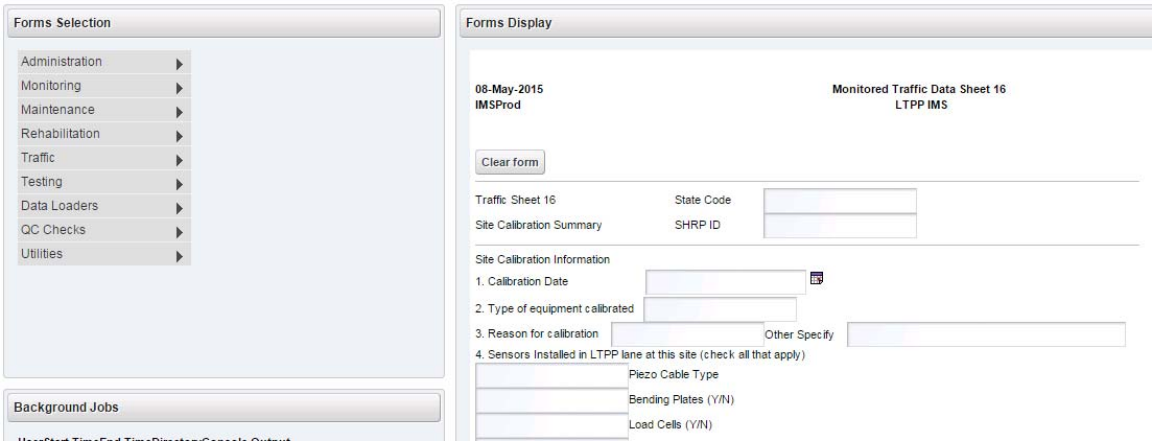


Figure 7. Screenshot. Sample PPDB form.

Much LTPP data has been collected on paper datasheets. In most cases, one datasheet represents one entry form. Entry forms were

designed to look like the datasheets to avoid mismatches of data being entered. Database tables were also designed to keep related data together. Most of the data from a particular datasheet is stored together in one table. Figure 7 shows a blank form for Traffic Data Sheet 16 entry located by clicking on Traffic under Forms Selection and then picking the Sheet 16 option.

Operations on a form are controlled by the permissions granted individual users.

Details on a form including content, format, codes, dependencies, minimum data checks (Level C QC), range checks (Level D QC), and intra modular checks (selected Level E QC) are available through the Field Definitions button at the bottom of each form.

iii. Scan Paper Data Sheets - Once paper data sheets have been reviewed and processed, they are scanned and filed in accordance with Directive I-170 or the most current version.

4. Assign Construction Number (CN) to Data Records -Each highway section included in the LTPP study has a documented pavement structure when it is accepted into the program. This structure is assigned a construction number (CONSTRUCTION_NO or CN) of 1. As maintenance and rehabilitation activities are performed on the section, the construction number is incremented and the changes are documented in the database. These changes are identified by the new construction number. CONSTRUCTION_NO is a key field in the EXPERIMENT_SECTION table, which contains one record for each STATE_CODE, SHRP_ID and CONSTRUCTION_NO combination. Occasionally, a rehabilitation event causes a section to move to a different experimental study or to go "out of study". For example, an AC overlay placed on a section in the GPS-1 study could move the section to the GPS-6B study.

   Since the pavement structure is critical to many types of pavement performance analysis, each data collection activity must be associated with the correct structure and the correct CN. Most data tables contain the CONSTRUCTION_NO field. As new maintenance or rehabilitation activities are added to the database, this field can get out of sync with the correct pavement structure for that data record. Therefore, a package of stored procedures has been developed to assign the correct CN to each data record by comparing the date of data collection to the date each CN was assigned to a given section.

   The CN assign procedure must be run before QC checks are performed on a module of data. The procedure can be run on demand from the Utilities menu in the Forms Selection section. CN Assign is also run nightly on the database.

5. Perform QC Checks - When new data has been entered or loaded into the LTPP database, a series of Quality Checks (QC) programs are run to check the

reasonableness of many of the data elements. Three types of checks are performed on the data.

- Level-C Checks – These are checks to identify critical fields that contain a null value.

- Level-D Checks - These are range checks on the validity and reasonableness of values entered in a field.

- Level-E Checks - These checks are relational checks between data stored in one field and data stored in other related fields or tables.

The RECORD_STATUS field in each table stores the quality status of each record. Records passing all level C checks are upgraded to RECORD_STATUS = C. Records passing level D checks are upgraded to D, and records passing level E checks are upgraded to E.

Not all data records will make it to level E. Some records will stay at a lower level until a revision to a QC program is distributed. Some records will not be upgraded because there is a question about the quality or correctness of the data.

QC programs are intended to run one level of QC checks at a time. Once level C has been run, the level C output is checked for errors, i.e., records that do not pass the checks. Records are corrected or upgraded as necessary, and level C QC is run again. Once the user is satisfied with the level C output, level D QC is run. Level D output is reviewed, corrections and upgrades are made and level E QC is run. Once level E output has been reviewed and the user is satisfied with the results, the QC process is complete.

a. Execute QC Programs -

b. Review QC Output - Each time a QC program is executed, an output file is generated listing each table and any records that did not pass the checks on that table. QC output files can be reviewed on-screen or can be printed. Files can be very large and should be checked for size before printing.

   All QC output has some general header information at the top of the file including date and time of run. For each database table with QC checks, the level C output has the table name and a column for each key field and for each "required" field. If a record is missing one or more required fields, the key fields are filled in and an "R" is placed in the columns for the missing field(s). *See ….. for a sample QC output files.*

   Level D QC output is formatted much like level C, except data elements that do not fall within the expected range are printed in the appropriate column. Level E output lists key fields for each error record and then an error message for each error encountered. Error messages are numbered to facilitate looking up the corresponding check in the QC Manual. The

QC Manual chapter corresponding to each data module is listed in table 2 and table 3.

c. Research Data Anomalies - QC output is used to identify records that have data anomalies. Sometimes, a data element is merely overlooked, mistyped or can be found or verified on the paper data sheet or in other documentation.

d. Correct or Manually Upgrade Data - A record that is listed in the level C QC output has not been upgraded to RECORD_STATUS = C by the QC program. This indicates that the record is missing one or more required fields. However, regional personnel may conclude that the missing data cannot be determined, but that the remaining data is still useful. In this case, the failing record can be manually (with SQL) upgraded to level C. Once all possible missing data is entered or records are manually upgraded, the level C QC can be rerun and the new output can be examined.

   Once the data manager is satisfied with the level C QC output, level D QC can be run. All records with RECORD_STATUS = 'C' that pass the level D checks will be upgraded to RECORD_STATUS = D. Level D output will be used to make corrections to the records that did not pass level D checks. In this case, a data value may have been mistyped or it may need to be removed because it is obviously wrong. However, if the data is correct and is just outside the expected range, the record can be manually upgraded to level D. Level D QC can be rerun to recheck and upgrade corrected records.

   Once the data manager is satisfied with level D QC output, level E QC is run. All records with RECORD_STATUS = 'D' that pass the level E checks will be upgraded to level E. Records that do not pass will be listed in the level E output and that will be used to make corrections and upgrades. Level E QC can be rerun to recheck and upgrade corrected records.

   Manual upgrades are performed using the Browser Application and QC output files to generate manual upgrade scripts for qualifying records. Refer to Browser documentation for more information on how to manually upgrade qualifying records.

6. Run Record Counts - The record count program (rec_cnt.exe) can be run on the PPDB at the regional or program level to create a report showing how many records in each data table have advanced to a record status of 'E'.

7. Populate AIMS Folders - Directive GO-I-170, or the most recent versions, also provides instructions on electronic format, file naming conventions, and directory

structure for the submission of files to the Ancillary Information Management System (AIMS).

APPENDIX A. ROLES AND RESPONSIBILITIES – TFHRC SERVER

The Disaster Recovery (DR) and Continuity of Operations Plan (COOP) appendices along with the "Data Processing Workstation IT Security Plan for the Long Term Pavement Performance Program" require that persons be identified to fulfill various roles. This section describes the roles required and the organizations providing individuals for those roles. The assignment of individuals by role and their contact information is provided by quarterly memo to the COR who is the Information System Owner. The contact information for the various organizations and individuals is also include. The information is provided separately from this document to remove personally identifiable information (PII) and prevent obsolescence of this document.

The role assignments for this system are reviewed quarterly. The organizations with people assigned to each role are documented in Table 4. Contact information for each organization is provided in Table 5.

- System Administrator - The system administrator is responsible for maintaining the TFHRC server in good working order. This includes the operating system, access control, installed software, backups, and hardware.

- Backup System Administrator - The backup system administrator is responsible for maintaining the TFHRC server under the direction of the system administrator and/or when the system administrator is unavailable. This includes the operating system, access control, installed software, backups, and hardware.

- TFHRC Database Administrator - The database administrator maintains the database instances on the TFHRC server. This includes database backups, schema modification, and storage management.

- Backup TFHRC Database Administrator - The backup database administrator maintains the database instances on the DPW. This includes database backups, schema modification, and storage management under the direction of the database administrator and/or when the database administrator is unavailable.

- TSSC Program Manager - The TSSC program manager is responsible for the oversight of the LTPP server activities at TFHRC.

- Technical Support Services Staff - The technical support services staff role provides support for TFHRC server activities on-site under supervision of the TFHRC database administrator.

- Customer Service - The Customer Service role is responsible for answering customer inquiries including distributing data. Customer Service is also responsible for maintaining some centrally processed data and maintaining copies of ADEP on the TFHRC server.

- TFHRC IT – The TFHRC IT role is responsible for granting VPN access through the FHWA TFHRC Internet 2 firewall and maintenance of FHWA licensed software.

- Information System Owner - The information system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

- Authorizing Official - The authorizing is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

- Assignment Of Security Responsibility - The assignment of security responsibility role is responsible for the overall security of the central server.

- Other Designated Contacts - The other designated contacts role designates key contact personnel who can address inquiries regarding system characteristics and operation.

- LTPP - The LTPP role provides FHWA oversight of the LTPP program.

Table 4. TFHRC server role assignments.

Role	**Organization with Individuals in the Role**
System Administrator	AMEC
Backup System Administrator	SAIC
TFHRC Database Administrator	AMEC
Backup TFHRC Database Administrator	SAIC
TSSC Program Manager	AMEC
Customer Service User	ESCINC
Technical Support Services Staff	AMEC
Information System Owner	FHWA
Authorizing Official	FHWA
Assignment Of Security Responsibility	AMEC
Other Designated Contacts	None
LTPP	See Team listing[1]
FHWA IT	TFHRC Help Desk

[1] http://www.fhwa.dot.gov/research/tfhrc/programs/infrastructure/pavements/ltpp/whoswho.cfm

Table 5. TFHRC Server - Organizational Contact Information.

Organization	Contact Information
Long Term Pavement Program Team (LTPP):	FHWA/DOT, HRDI-30 6300 Georgetown Pike McLean, VA 22101
TFHRC IT:	FHWA/DOT, HRRM-1 6300 Georgetown Pike McLean, VA 22101
SAIC:	151 Lafayette Drive Oak Ridge, TN 37830
AMEC Environment & Infrastructure (AMEC):	12000 Indian Creek Court, Suite F Beltsville, MD 20705 (301) 210-5105
Engineering & Software Consultants, Inc. (ESCINC)	14123 Robert Paris Court Chantilly, VA 20151

APPENDIX B. CONTINUITY OF OPERATIONS – TFHRC SERVER

PURPOSE

The Continuity of Operations Plan (COOP) describes how the Long Term Pavement Performance (LTPP) Program will continue to function when the TFHRC server is unable to sustain normal operations. The outage may be partial or total and may be the result of operator error, software problems, hardware problems, or network connectivity problems.

Scope

The scope of this COOP is the TFHRC Server.

Situation Overview

The THFRC server is used for the central archival of data gathered by the regional contractors. It provides the source of data disseminated to the public through standard media formats and on demand requests. Original copies of the data are maintained on the DPW and within the regions. Because the original data is not lost, it is possible for the THFRC server to be unavailable for a period of time without causing all data dissemination activity to stop. The primary risk to the system being unavailable is that delivery of data may be delayed beyond scheduled dates.

Planning Assumptions

The LTPP Team has agreed that three days of downtime would not have an adverse effect on data delivery. It has also been decided that if a hardware problem occurs with the server, the server will be repaired. Therefore there is not a failover system standing by. As explained later, we will rely on the Dell server maintenance and support agreement to repair the system in the event of a hardware failure.

Objectives

The objective of this plan is to outline the steps necessary to minimize disruption to LTPP data delivery in case of a system failure.

CONCEPT OF OPERATIONS

Phase I: Readiness and Preparedness

Knowing that system failures are inevitable, there are certain steps that can be taken ahead of time to ensure that services can be restored in a timely manner.

Backups

The server contains two Redundant Array of Independent Disks (RAID) volumes. The first volume is configured as a RAID 1 array consisting of two 1 TB Serial-Attached

Small Computer System Interface (SAS) drives. This volume is the C: drive and contains the operating system as well as a copy of the database backups, source code repository, and archive logs. This drive also hosts the bulk of the web applications. The RAID 1 array can withstand a single drive failure and remain operational. These drives are not hot swappable. The second volume is configured as a RAID 5 array consisting of seven 2 TB SAS drives. There is an eighth 2 TB SAS drive standing by as a hot spare. This array can withstand a single drive failure and the hot spare will automatically take the place of the failed drive providing additional protection until the failed drive can be replaced. These drives are hot swappable. This array is the D: drive and contains the database instances, ADEP repositories, and backup staging areas.

The diagram below shows the highlights of the backup process.

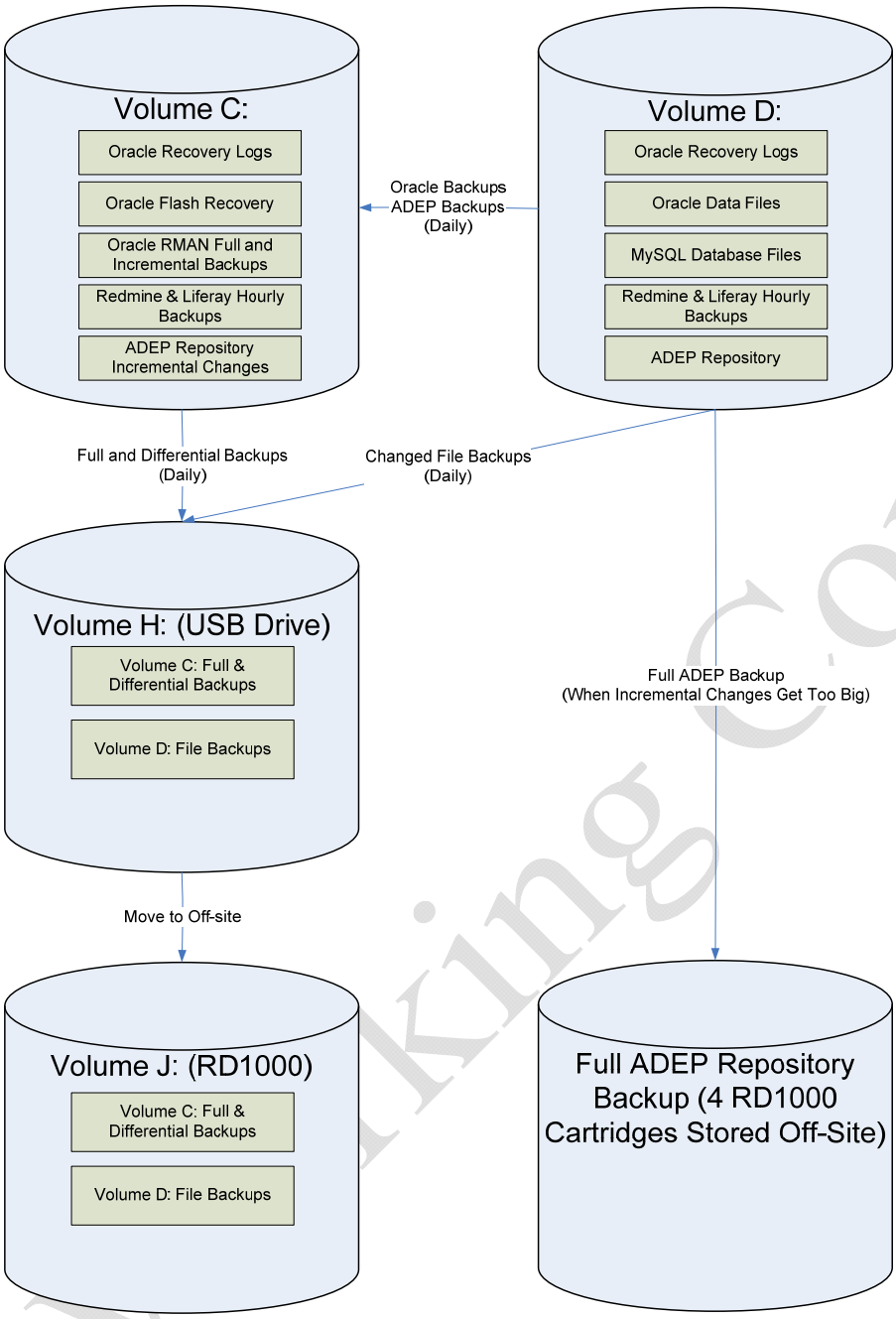


Figure 8. Schematic - Backup Process Overview – Replace with TFHRC equivalent or reference to backups section of backups and archives.

Drive Backup Strategy

The Seagate Backup Plus mounted on drive J: is used to write backups for off-site storage. The system uses 4TB drives for working off-site backups. A 4TB external hard drive mounted on Drive M: is used for incremental backups.

There are multiple types of backups taking place. *First, there are the drive level backups. Symantec Backup Exec System Recovery 2010 is used to back up drive C: to the staging area H:\SymantecRecoveryPoints. The backup of drive C: starts with a full image backup on Sunday at 10:30 PM with differential backups created at 10:30 PM Monday through Saturday. The staging area maintains two full image/differential backup sets. The Backup Exec software also takes care of copying the current week's backup files to drive J: to be moved off-site. This copy occurs as the full or differential backup completes. The backup of drive D: is handled differently since the backup media is not large enough to contain an image backup. Drive D: is backed up on a file by file basis to H:\SymantecRecoveryPoints\LTPPDPW using Symantec Backup Exec 2010. There are several directories that are excluded from the backups such as the ADEP repositories and the LTPP database instances. This backup is scheduled to run every day at 11:30 PM. The backup job does not automatically copy files to drive J: for off-site storage when complete. There is a Windows Task Scheduler job (CopyIncrementalFileBackupToCartridge) that copies the H:\SymantecRecoveryPoints\LTPPDPW directory to J:\LTPPDPW at 6:00 PM every day.*

Application Backup Strategy

The majority of the application on the server are COTS and installed on C:\. LTPP Specific applications are not developed on the server. The backup period for LTPP applications run on the server is linked to the Oracle backup cycle.

Oracle Database Instances

The control files and redo logs are written to drives D: and K:\ in \LTPP_Database\<instance> where <instance> is IMSProd, IMSTest, or IMSDev. The control files contain the latest structure of the database files and the redo logs contain the latest transactions. Drive K: contains the Flash Recovery Area in *K:\LTPP_Database\<instance>\FlashRecoveryArea and the Archive Logs in C:\LTPP_Database\<instance>\ArchiveLogs. If drive C: fails, drive D: contains all of the files necessary to recover the database. If drive D: fails, the RMAN backups from drive C:'s Flash Recovery Area will need to be restored and the logs applied in order to recover the database. Redo logs and archive logs are managed by the Oracle instance and allow recovery of the last transaction committed before the failure. The RMAN backups are managed by two Windows Task Scheduler jobs. The "RMAN Level 0 Backup" runs every Tuesday at 6:00 AM. This job produces a full backup of the instance and removes old archive logs and backup sets that are no longer necessary. The "RMAN Backup" runs every day at 10:00 PM. It produces a differential backup of changes to the data base instances. The drive C: backup captures these backups for off-site storage.*

AIMS Repository and Historical Files

The AIMS Repository and historical files are too big to fit onto a single cartridge. As a complete copy of the AIMS exists on an external hard drive in the possession of Customer Service in addition to the copy on the DPW, the decision has been made not to backup

video files. A full backup strategy has been implemented for all other files. The AIMS repositories reside in K:\Historical_AIMS\<YYYY> where <YYYY> is year of the update. The backups are done the 1st Wednesday of February, May, August and November of each year and run for more than 24 hours due to the inclusion of the verify option in Symantec Backup Exec 2015.

Recovery Media

The DVDs required to rebuild the server are located in server room in the top right drawer of the credenza. Return of off-site backups can be requested from First Federal Corporation. The information system owner would be the primary person to interface with First Federal Corporation. The system administrator would be the secondary contact.

Dell Service

The TFHRC server is a Dell PowerEdge R515 with service tag 5XT8J02. It is covered by the "Gold or ProSupport with Mission Critical" and the "4 Hour On-Site Service" plans until 5/10/2019. These warranty plans ensure that the TFHRC server will be repaired quickly. The system administrator would be the primary person to interface with Dell Support. The information system owner would be the secondary contact.

The two MD1200 40 TB storage units with service tags J3BVFZ1 and 2SFVL02 are under warranty until 5/17/2017.

Phase II: Activation

Decision Process

The decision to implement will begin with the initial notification that the server is not functioning. This will typically be on direct observation by the system administrator. Upon identification, the severity of the problem will be assessed. If it is determined that the problem can likely be resolved by a restart of services, then those actions will be taken before implementing this plan.

Alert and Notification

If it is determined that actions beyond a quick fix, the information system owner and the TSSC program manager will be notified in person, by phone or by e-mail as appropriate . This notification will include any details that are known about the outage along with an expected duration if it is known. This notice should be followed up with additional emails as details become available. Finally, notice should be sent when the system is available for use.

Phase III: Continuity Operations

Essential Functions

The essential function of data archival can continue with only a slight degradation. This is because the there are at least two other off-site copies of the information on the TFHRC server. Data extraction for general dissemination occurs during the March through April time frame which is the most critical period for on-line functionality. Down time primarily affects schedules in the extraction and review process. Data extraction on request is a process that occurs in low volumes sporadically throughout the year. Most responses are associated with material not available through InfoPave. The few requests that cannot be handled with the SDR require access to AIMS and can be addressed with the copy maintained by Customer Support. Downtime primarily affects turnaround time on a response.

Essential Personnel

- Order of Succession
    - System Administrator
    - Information Systems Owner
    - FHWA IT
- Delegation of Authority

Essential Equipment and Systems

- PowerEdge R515 (TFHRC Server)
- 2 MD1200 40TB storage units
- Seagate Backup Plus 4TB External Hard Drives
- Connection to the internet
- Installation Media

Continuity Facilities

Resumption of operations in the event of a catastrophic failure at the TFHRC facility will follow the plan for the facility as a whole.

Continuity Communications

There is not another connection to the internet designated for resuming operations in the event of a catastrophic event at the TFHRC facility. Communications between personnel will be accomplished using a combination of phone and email.

Phase IV: Reconstruction Operations

The plan is to repair current systems to restore service. This will be accomplished using vendor support such as the Dell on-site service contract along with THFRC systems personnel to restore the THFRC server with the least data loss possible. When the THFRC is ready to be used for data dissemination, a notice will be sent to the contacts listed in the Alert and Notification section.

APPENDIX C. DISASTER RECOVERY – TFHRC SERVER

INTRODUCTION

Purpose

The purpose of the disaster recovery plan is to define a set of potential problems and their likely solution.

Planning Assumptions

The basic assumption is that there is a three day window to recover from a disaster without causing serious disruption in data dissemination capabilities. Given that a hot standby is not required, it has been decided that the most cost effective solution is to repair whatever is wrong with the current system and resume operations. We are counting on the Dell ProSupport Mission Critical Option that specifies 4 hour on-site service with 6 hour parts availability to resolve any hardware problems with the TFHRC server. We are also counting on First Federal Corporation to be able to deliver backups from off-site storage within three hours of an emergency request.

Objectives

The main objective is the restore the TFHRC to full operational status as soon as possible with minimal data loss. A secondary objective is to keep key personnel at the FHWA, and the TSSC informed about the problem and its resolution. When possible, limited functionality will be made available while permanent repairs are underway.

Concept of Operations

SYSTEMS OVERVIEW

The TFHRC server is a databases and files housed on a single server that is accessible either on location or via VPN. As shown in Figure 9 a keyboard connected via a KVN switch and VPN are the primary entry points into the system.

Insert figure here.

Figure 9. Schematic. TFHRC Server Access Diagram

Risk Identification and Mitigation

Internet Connection Failure

- Description -An internet connection failure will first become apparent due to failure to access the system via VPN or access to sites for update of the OS and anti-virus software.

- Effect - The effect is that the server appears to be down for external access. There will be no remote connection capability. On the server side, everything is functioning normally and access will return as soon as the internet connection is restored.

- Mitigation - There are no workarounds to allow the user access to the server.

- Resolution - Notify TFHRC IT that the VPN network is down for external access failures either inbound or outbound. This step is typically unnecessary since they have automated notifications when the VPN network has a problem. Wait for service to be restored.

TFHRC Software Services Become Unresponsive

- Description - Software services becoming unresponsive typically results in inability to access an Oracle instance.

- Effect -The effect is that users are prevented from using the affected Oracle instance.

- Mitigation - No mitigation is necessary.

- Resolution – If resources were not the problem, check table 6 to determine which service needs to be restarted. On rare occasions, a restart of the central server may be required.

Table 6. TFHRC server Oracle service diagnostics.

Service	***Description***
OracleOraDb11g_home2TNSListener	This listens for connections to the Oracle database instances. Restart this service if having Oracle connection problems. Restarting this service will typically not impact users greatly. Restart takes about 30 seconds.
OracleServiceIMSDEV	This is the **development** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSPROD	This is the **production** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSTEST	This is the **test** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.

Single Hard Drive Failure on the RAID 1 Array

- *Description - A single drive failure on the RAID 1 array (C:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.*

- *Effect - There is no effect on server operations.*

- *Mitigation - No mitigation is possible.*

- *Resolution - Contact Dell Support and declare this a severity 1 critical situation because if the other internal drive fails before the bad drive is replaced and had time to rebuild, the entire system volume is lost. This will cause the server to be unavailable until the drives are replaced and reloaded from backups.*

  A 30 minute to 1 hour down time will be required to replace the failed drive when the replacement arrives. After the replacement, there could be a period of several hours where performance is degraded due to the mirror being rebuilt.

Single Hard Drive Failure on the RAID 6 Array

- *Description - A single drive failure on the RAID 6 array (D:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.*

- *Effect - There is no effect on server operations.*

- *Mitigation - The hot spare will take the place of the failed drive. There are a few hours while the hot spare is being built where server performance may be degraded and the loss of an additional drive could cause the loss of the array.*

- *Resolution - Contact Dell and have them ship a replacement drive under warranty. When the replacement arrives, hot swap the failed drive and the replacement. The replacement drive will become part of the array and the hot spare will go back to its role as a standby. There may be a few hours of degraded performance while the replacement drive is being rebuilt.*

Failure of the RAID 1 Array

- *Description - A failure of the RAID 1 array (C:) would take down the server. The system will not boot.*

- *Effect - Because the operating system is on C:, the system would not be able to continue operations and it would be impossible to reboot the server due to the lack of a boot drive.*

- *Mitigation - A copy of the latest drive C: backup is kept on an attached USB drive as well as removable RD1000 cartridges.*

- *Resolution - Contact Dell and have them determine the cause of the failed array. After the failed drives and/or controllers are replaced, install the OS, anti-virus and Symantec Backup Exec 2015. From there, you can restore the latest usable backup. The Oracle instances will likely need recovery after drive C: is restored due to the sudden crash of the operating system. The expected downtime would be 1 to 2 days.*

Failure of the RAID 6 Array

- Description - *A failure of the RAID 5 Array (D:) would leave the server running, but the portals, Redmine, LTAS, APEX, and ADEP would be unavailable because they depend on database repositories on D:. The code repositories would still be accessible if needed.*

- *Effect - Files on D: will be unavailable. There will also be a loss of data due to some files not being backed to stay within the limitations of our backup media. The files that will be lost are not critical to operations.*

- *Mitigation - A copy of the latest drive D: backup is kept on an attached USB drive as well as removable RD1000 cartridges.*

- *Resolution - Contact Dell and have them determine the cause of the failed array. After the failed drives and/or controllers are replaced, copy the files from the latest backup onto the D: drive. It will also be necessary to have the four cartridges that make up ADEP backup returned from Iron Mountain off-site storage. The contents of those cartridges will need to be copied onto D: and then the incremental backups from drive C: will need to be applied to restore ADEP to a point that is within 1 day of the crash. The Oracle database instances will need to be restored from the RMAN backups on C: and the logs applied to roll the databases forward until the point that the Array failed. If for some reason the MySQL instance does not come up, it can be recreated using the backups located in C:\backup. The expected downtime would be 2 to 3 days. Most services could be restored by the second day with ADEP being the last service to come back online.*

Complete Loss of Facilities at TFHRC

- Description - This would be a catastrophic event that completely destroys the facilities at TFHRC along with the server and on-site backups.

- Effect - No services provided by the TFHRC server would be available.

- Mitigation - Off-site backups stored outside of TFHRC.

- Resolution – Retorign the server would follow the facility plan for restoring THFRC facilities. The latest off-site backups would be shipped to FHWA designated facility where the external USB drives could be used to apply the

backups to a Windows 2008 R2 server built in the Amazon cloud. The expected downtime would be approximately a week. This largely depends on FHWA TFHRC's recovery procedures.

APPENDIX D. HARDWARE MAINTENANCE

The following guidelines are provided to assist in checking the TFHRC server for problems before they result in data loss. It is recommended that the visual checks be performed on at least a weekly basis, concurrent with the server backup process. Checking the operational status of various server components can be done using the DRAC as discussed at the end of this appendix. This should be done at least monthly.

The server is designed to be somewhat fault tolerant. It features multiple power supplies and hot swappable hard drives. While the uptime requirements of the central server are not that high, this redundancy helps to keep the systems running while waiting on parts to arrive. On the down side, without someone checking the system for faults on a regular basis, the server can keep running for a long time with failed parts. This can lead to a loss of data if, for example, one hard drive has already failed and another fails before the first failure is repaired.

Hardware status is determined on a gross level by visual inspection as discussed in the following sections. The hard drives, power supplies, and the codes on the LCD panel should be checked at least once a week.

The hard drives are joined together in a single RAID 6 array. The hard drives are partitioned into volumes and these volumes are set aside for different purposes. Microsoft Windows Server is installed on the C: volume. The Oracle database files are stored on the D: volume.

SERVER

The central server is a Dell PowerEdge™ R515 with two 3 GHz Xenon E5450 quad-core processors. It is a twelve bay system, eight of which are populated with 4TB 7,200 RPM near-line SAS hot plug drives. *This server also has 32 GB of RAM, an internal RAID 5 Array consisting of eight 7,200 RPM 1-TB SATA disks.* There are two attached external twelve.bay MD1200 storage units discussed separately. For backups, it has 4TB external USB 3.0 hard drives. All of this is protected by a 2200 VA UPS.

The server setup for the Dell R515 is detailed in …...doc (see Appendix T. Reference Documents.) This document describes in detail how the RAID Array, operating system and Oracle databases were configured.

The *Dell PowerEdge R515 Systems Hardware Owner's Manual* is stored in the Dell subdirectory of the D:\ScratchSpace\Software_Downloads folder. A second copy is stored on the incremental backups hard drive in the folder Setup\Manuals.

Server status

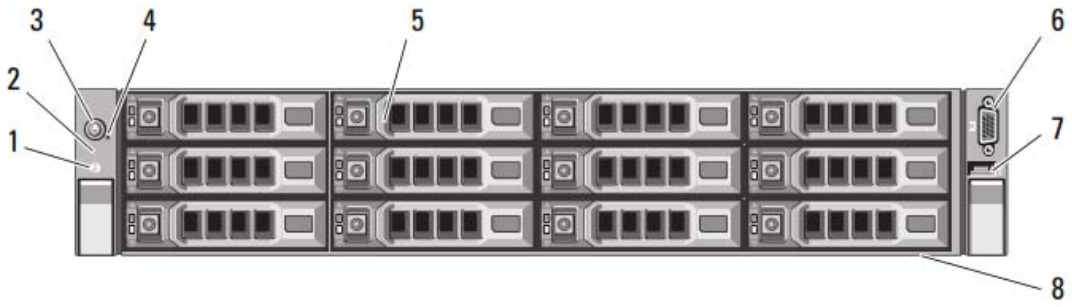
The basic procedure is to look for lights that are not green/blue on the front of the server. Each hard drive should have a green drive-status indicator. Each power supply should have a green power supply status and a green AC status indicator. And as a general

check, the LCD panel should be blank. If anything goes wrong on the system, the LCD panel will have one or more lit numbers indicating what further action is necessary. The back of the server should be checked to verify that all of the lights associated with the storage to server connections are on and green.

The following sections contain excerpts from the *Dell PowerEdge R515 Systems Hardware Owner's Manual*[1].

Front Panel Inspection

Figure 10 shows the front panel features of the Dell R515. The LTPP unit uses only eight bays.



1	System identification button	2	Diagnostic lights
3	Power-on indicator/power button	4	NMI button
5	Hard drives	6	Video connector
7	USB Connector (2.0 compliant)	8	System identification panel

Figure 10. Illustration[2]. Front panel features.

The power button on the front panel controls the power input to the system's power supplies. The power indicator lights *green* when the system is on.

The hard-drive carriers have two indicators — the drive-status indicator and the drive-activity indicator (Figure 11). Each existing hard drive should have a green drive-status indicator.

[1] http://www.dell.com/support/home/us/en/19/product-support/servicetag/5XT8H02/manuals, accessed 5/6/2015.

[2] Image taken from *Dell PowerEdge R515 Systems Hardware Owner's Manual*.

1	drive-status indicator (green and amber)	2	green drive-activity indicator

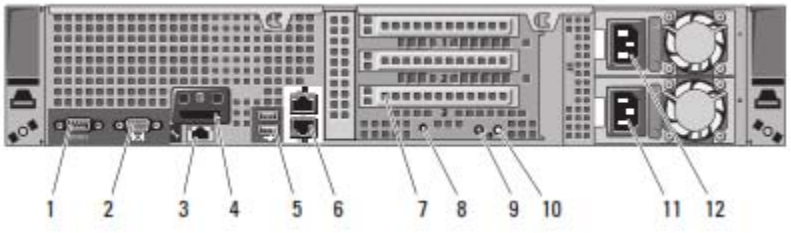
Figure 11. Illustration2. Hard drive carrier.

Table 7 lists the drive indicator patterns. Different patterns are displayed as drive events occur in the system. For example, if a hard drive fails, the "drive failed" pattern appears. After the drive is selected for removal, the "drive being prepared for removal" pattern appears, followed by the "drive ready for insertion or removal" pattern. After the replacement drive is installed, the "drive being prepared for operation" pattern appears, followed by the "drive online" pattern.

Table 7. Hard-drive indicator patterns.

Condition	**Drive-Status Indicator Pattern**
Identify drive/preparing for removal	Blinks green two times per second
Drive ready for insertion or removal	Off
Drive predicted failure	Blinks green, amber, and off.
Drive failed	Blinks amber four times per second.
Drive rebuilding	Blinks green slowly.
Drive online	Steady green.
Rebuild aborted	Blinks green three seconds, amber three seconds, and off six seconds.

Back Panel Inspection



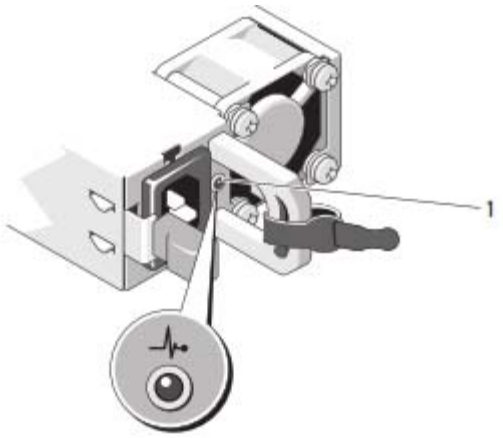
1	Serial connector	2	Video connector
3	iDRAC6 Enterprise port (optional)	4	VFlash media slot (optional)
5	USB connectors (2 – USB 2.0 compliant)	6	Ethernet connection (2 – 10/100/1000)
7	PCI expansion slots using riser card	8	System identification connector
9	System status indicator	10	System identification button
11	Power supply 2	12	Power supply

Figure 12. Illustration. R515 back panel.

The indicators on the optional redundant power supplies show whether power is present or whether a power fault has occurred (see table 8 and figure 13).

Table 8. Function of redundant power supply indicators.

Color	**Condition**
Not lit	AC power not connected
Green	In standby mode, indicates that a valid AC source is connected to the power supply and that the power supply is operational..
Amber	Indicates a problem with the power supply.
Alternating green and amber	Mismatched power supplies when hot adding a power supply.



1	power supply status

Figure 13. Illustration2. Location of redundant power supply indicators.

Diagnostic Light Codes

The system's front panel displays error code during startup. The diagnostic lights are not lit after the system successfully boots to the operating system. Table 9 provides a list of codes and the location in the owner's manual for further troubleshooting.

Table 9. Diagnostic light codes Dell R515.

Code	Causes	Corrective Action
①②③④	The system is in a normal off condition or a possible pre-BIOS failure has occurred.	Plug the system into a working electrical outlet and press the power button.
①②③●	BIOS checksum failure detected; system is in recovery mode.	See "Getting Help" on page 187.
①②●④	Possible processor failure.	See "Troubleshooting Processors" on page 174.
①②●●	Possible expansion card failure.	See "Troubleshooting Expansion Cards" on page 172.
①●③④	Memory failure.	See "Troubleshooting System Memory" on page 165.
①●③●	Possible video failure.	See "Getting Help" on page 187.
①●●④	Hard drive failure. Ensure that the diskette drive and hard drive are properly connected.	See "Hard Drives" on page 87 for information on the drives installed in your system.
①●●●	Possible USB failure.	See "Troubleshooting a USB Device" on page 158.
●②③④	No memory modules detected.	See "Troubleshooting System Memory" on page 165.
●②③●	System board failure.	See "Getting Help" on page 187.
●②●④	Memory configuration error.	See "Troubleshooting System Memory" on page 165.

Code	Causes	Corrective Action
	Possible system board resource and/or system board hardware failure.	See "Getting Help" on page 187.
	Possible system resource configuration error.	See "Contacting Dell" on page 187.
	Other failure.	Ensure that the optical drive, and hard drives are properly connected. See "Troubleshooting Your System" on page 157 for the appropriate drive installed in your system. If the problem persists, see "Getting Help" on page 187.

Dell Support – Server

All equipment was purchased with Dell Support. Terms and information needed to obtain support follow.:

- Model: Dell PowerEdge R515
- Service Tag: 5XT8H02
- Express Code: 121928399634

The contact information for Dell is www.dell.com/ProSupport Federal Government under support if doing troubleshooting or requesting help. Phone: 1-800-945-3355. A Service Tag will be needed when calling.

Customer Acct: 20080702

Customer Purchase Order #: DTFAWA-11-D00004

Dell Purchase ID:

Order Number: 1200337526

Server maintenance and support are as follows:

Dell Hardware Warranty Plus Onsite Service Initial Year

Dell Hardware Warranty Plus Onsite Service Extended Year(s)

ProSupportPlus (www.dell.com/prosupport/regionalcontacts) - April 9, 2014-April 10, 2019

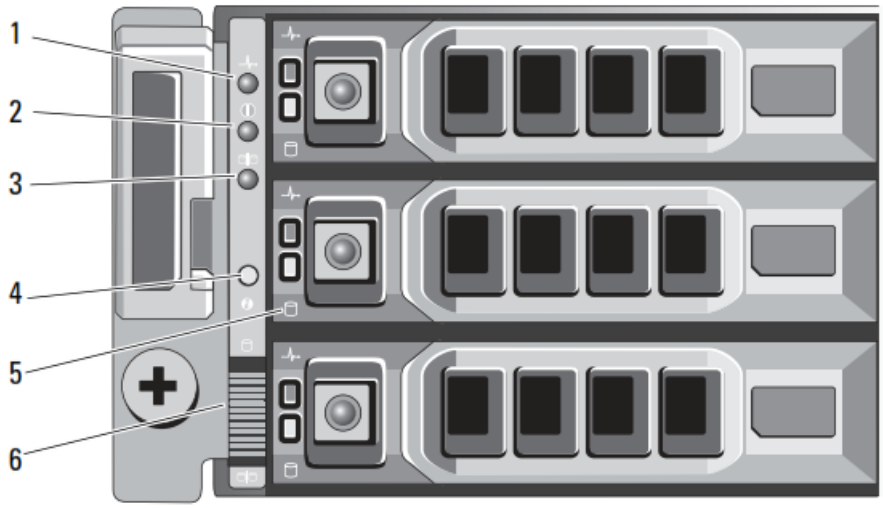
4-hour 7x24 On-site service with Emergency Dispatch, Initial Year

4-hour 7x24 On-site service with Emergency Dispatch, 4 Year Extended – April 10, 2015 – April 10, 2019

ATTACHED STORAGE

There are two attached external twelve bay MD1200 storage units discussed separately. Each unit is populated with ten 4TB 7,200 RPM Near-line SAS 3.5 inch hot pluggable drives. Documentation[3] is stored in the Dell subdirectory of the D:\ScratchSpace\Software_Downloads folder. A second copy is stored on the incremental backups hard drive in the folder Setup\Manuals.

Figure 14 shows the elements and indicators on the front of the storage units. The enclosure status LED should be blue indicating normal operation. If the light is amber after the unit is turned on, an error exists. The drives are hot swappable and should be lit with blue lights under normal operation.

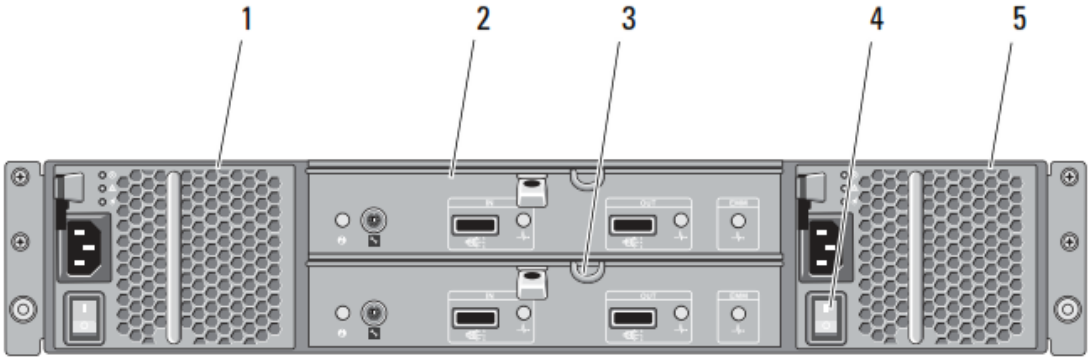


1	Enclosure status LED	2	Power LED
3	Split mode LED	4	System identification button
5	Hard drives	6	Enclosure mode switch

Figure 14. Illustration[4]. Front view of Dell PowerVault MD1200.

[3] http://www.dell.com/support/home/us/en/04/product-support/product/powervault-md1200/manuals, accessed 5/7/2015.

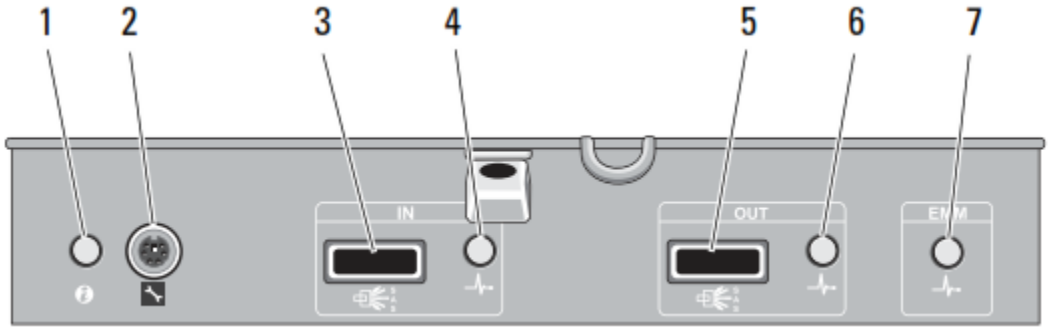
[4] Image taken from Dell™ PowerVault™ MD1200 and MD1220 Storage Enclosures Hardware Owner's Manual



1	Power supply/cooling fan module	2	Primary enclosure management module (EMM)
3	Secondary enclosure management module (EMM)	4	Power switches (2)
5	Power supply/cooling fan module		

Figure 154. Illustration. Rear of MD1200 unit.

Comments on status indicators good and bad.



1	System status indicator	2	Debug port
3	SAS port (In)	4	In port link status
5	SAS port (Out)	6	Out port link status
7	EMM status LED		

Figure 164. Elements of Enclosure Management Module.

Dell Support - Storage

All equipment was purchased with Dell Support. The equipment is under warranty. If Dell needs to be contacted the following information may be useful:

- Model: Dell PowerVault MD1200
- Upper unit:
    - Service Tag: J3BVFZ1
    - Express Code: 41560205725
- Lower unit:
    - Service tag: 2SFVL02
    - Express Code: 6073285394

The contact information for Dell is www.dell.com/ProSupport Federal Government under support if doing troubleshooting or requesting help. Phone: 1-800-945-3355. A Service Tag will be needed when calling.

Customer Acct: 20080702

Customer Purchase Order #: DTFAWA-11-D00004

Dell Purchase ID:

Order Number: 1200337526

Maintenance and support are as follows:

Dell Hardware Warranty Plus Onsite Service Initial Year

Dell Hardware Warranty Plus Onsite Service Extended Year(s)

ProSupport: Next Business Day, Initial Year

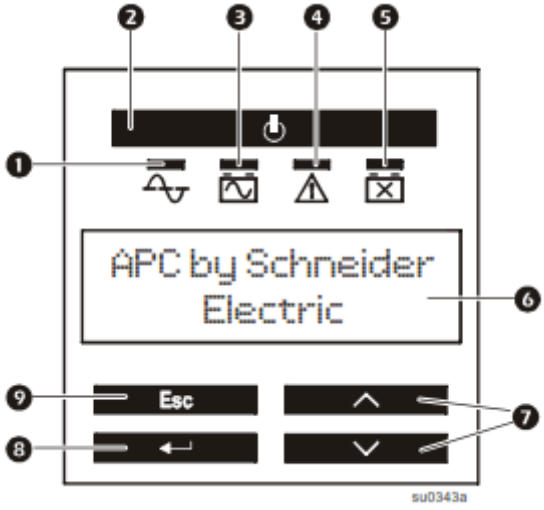
ProSupport: Next Business Day, 2 Year Extended, 3/26/2015 to 3/26/2017

UPS

The UPS for the Dell R515 is an APC Smart UPS 2200 (figure 17), rack mount. It is the upper of the two UPS units in the server rack.

Figure 17. Photos[5]. APC Smart UPS 2200 rack mount UPS front and back SMT model.

The model number is SMT2200RM2U. The serial number is AS1403141091. The unit has a three year repair and replace on all elements except for the battery. There is a two-year warranty on the battery. The effective date of the warranty is the manufacturing date, January 14, 2014. In the event of battery failure, a single replacement battery, model RBC43, will be required.



[5] From http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=SMT2200RM2U&total_watts=50, accessed 5/7/2015.

1	Online LED	2	UPS On/Off key
3	On Battery LED	4	Site Wiring Fault LED
5	Replace Battery LED	6	Display interface
7	Up/Down arrow keys	8	Enter key
9	Escape key		

Figure 18. Illustration[6]. SMT 2200 Smart UPS front panel.

Documentation[7] is stored in the APC subdirectory of the D:\ScratchSpace\Software_Downloads folder. A second copy is stored on the incremental backups hard drive in the folder Setup\Manuals.

The front display panel is shown in figure 18. The system status can be determined by checking the LEDs and reviewing the menus on the display panel. There are both Standard and Advanced menus. Under the Standard menue are Status, Configuraiton, Test and Diagnostics and an About Function. The up and down keys are used to scroll through the menus. Pressing enter permits viewing the submenus.

DRAC USAGE

The DRAC or Dell Remote Access Card provides a visual interface to check on hardware components including batteries, power supplies, controllers, hard drives, and fans.

[6] Illustration from Operation Manual, Smart-UPS™ Uninterruptible Power supply, Rack-Mount 2U, 750/1000/1500 VA 120/230 Vac; 2200 VA `120 Vac; 3000 VA 100/120/208/230 Vac

[7] http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=DLA2200RM2U&tab=documentation, accessed 5/7/2015.

APPENDIX E. BACKUP POLICIES

BI-WEEKLY DRIVE ROTATION SCHEDULE

*The drive rotation for weekly backups is the 13 week schedule discussed in Inputs to Backup Policies. In figure 19 the schedule for 2015 taken from the offsite_rotations spreadsheet is provided. The underlined dates are the weeks that off-site pickup and delivery occurs. The Week column is the number of the week in the quarter. The Date value is the Tuesday backup date. The Tape number is the label on the box and the tape of the tape to be used. When a tape other than the 2-year archive is taken out of the rotation, it is replaced by a tape with the same number and an alpha character. The off-site column indicates whether or not the tape is sent off-site for storage. It is sent out the following month the indicated Thursday date. The Recycle date is the date that a tape will be reused. It has only been filled in for tapes sent off-site so that the date it needs to be returned from storage can be identified. The recycle date in all cases is the Date value on which the tape is used the next quarter. Tapes identified with an * (asterisk) are on a 2-year archive schedule and the year for recycling is 2012 for the 1st 3 quarters and 2013 for the 4th quarter.*

Full weeklies

Week	Date	Tape	Off-sit	recycle	return	Date	Tape	Off-site	recycle	return	Date	Tape	Off-site	recycle	return	Date	Tape	Off-site	recycle	return
1	5-Jan	1	N			6-Apr	1				6-Jul	1				5-Oct	1			
2	12-Jan	2	N			**13-Apr**	2				**13-Jul**	2				12-Oct	2			
3	**19-Jan**	3	N			20-Apr	3				20-Jul	3				**19-Oct**	3			
4	26-Jan	4	18-Feb	27-Apr-10	15-Apr-10	27-Apr	4	20-May-10	27-Jul-10	15-Jul-10	27-Jul	4	19-Aug-10	26-Oct-10	21-Oct-10	26-Oct	4	18-Nov-10	25-Jan-11	20-Jan-11
5	2-Feb	5	N			4-May	5				3-Aug	5				2-Nov	5			
6	9-Feb	6	N			11-May	6				10-Aug	6				9-Nov	6			
7	**16-Feb**	7	N			**18-May**	7				**17-Aug**	7				**16-Nov**	7			
8	23-Feb	8	18-Mar	25-May-10	20-May-10	25-May	8A	17-Jun-10	24-Aug-10	19-Aug-10	24-Aug	8A	16-Sep-10	23-Nov-10	18-Nov-10	23-Nov	8A	16-Dec-10	22-Feb-11	17-Feb-11
9	2-Mar	9	N			1-Jun	9				31-Aug	9				30-Nov	9			
10	9-Mar	10	N			8-Jun	10				7-Sep	10				7-Dec	10			
11	**16-Mar**	11	N			**15-Jun**	11				**14-Sep**	11				**14-Dec**	11			
12	23-Mar	12	15-Apr	20-Mar-12	15-Mar-12	22-Jun	Bnew	15-Jul-10	26-Jun-12	21-Jun-12	21-Sep	13				21-Dec	13			
13	30-Mar	13	N			29-Jun	13				28-Sep	Cnew	21-Oct-10	27-Sep-12	20-Sep-12	28-Dec	Dnew	20-Jan-11	25-Dec-12	20-Dec-12

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive

The first date on the sheet is the 1st Tuesday of the year

All successive dates are prior +7

Tape from 4th Tuesday goes off-site

Off-site date is backup date + 23 (3 weeks plus 2 days W, R)

Recyle date is date is 13 weeks for tapes done in any month but 3, 6, 9, 12

Recyle date is date is 2 years for tapes done in months 3, 6, 9, 12

Return date is pickup date for month prior to recycle date for all tapes

Return date has been set so tapes do not have to be swapped when containers are recycled.

Calendar can be extended by copying the page and resetting the 1st January date to the 1st Tuesday of the year.

The tapes names for the quarterly 2yr holds change every year. 12, B, C, D in the even calendar years, E, F, G, A in the odd years

Adjustments will need to be made for leap year (2012)

2 yrs due back	
12	15-Mar-12
Bnew	21-Jun-12
Cnew	20-Sep-12
Dnew	20-Dec-12

Figure 19. Screenshot. Bi-weekly tape rotation for 2015.

QUARTERLY TAPE ROTATION SCHEDULE

The quarterly tape rotation schedule addresses the backups of AIMS material, annual submissions and the indefinite archives.

INPUTS TO BACKUP POLICIES

This material is derived from the FHWA July 2009 backup procedures document. This system does not include indefinite archives. Indefinite archives are covered in the annual data submission and the NARA submission.

The frequency of backup to cartridge by server drive has been established based on drive usage. The inclusion of incremental backups for drives backed up weekly to cartridge was initiated when additional "external" storage was installed.

Table 10. Database Server Frequencies

Drive Letter	Partition Name	Total GB	Update Cycle	Backup Frequency
C:	OS	40	Continuous	Weekly
D:	Working Storage	1,710	Continuous	Incremental #1 Weekly
E:	AIMS	1,710	Quarterly	Last and first quarter of year
F:	Traffic	1,210	Annual	Quarterly
G:	Database	,1670	Annual for core data (uploads); Continuous for analysis	Incremental #2 Weekly
H:	Recovery	3	Never. Dell recovery area.	Never
var	USB port		N/A – drives connected for upload of data	
J:	Backup device		N/A – backup cartridges	
K:	Archive	50,000	N/A – primarily backup area; Some materials have external drive backup on a topic specific basis	

The following is the "ideal" 13 week cycle using following logic:

A minimum of 13 weeks exists between reuse of a cartridge

Every 4th cartridge used is stored off-site for a 13-week period

Off-site storage occurs 2-weeks after the backup occurs

A recycled cartridge from off-site is used the week after it returns from storage

The last backup of a calendar quarter is stored off-site for 2 years before recycling

A new cartridge is used for each backup stored off-site for 2 years for the 1st two years. This is cartridge #12 for the 1st 2-year backup and A-G for the next 7 in the cycle.

The ideal cycle has been modified because cartridge pickups are a fixed week of the month and not a fixed interval. A spreadsheet, offsite_rotationsNN.xls, saved in G_Task Order 1…\Task_D_IMS_Hardware-Software\1_Database Operation\a_Operating the Database\0_Backup_Procedures was used to develop the annual calendar and container rotation schedules for the various backups. The modification has been designed to avoid, to the extent possible, swapping backup cartridges in and out of storage boxes at the time of pick up.

The 13 week cycle implemented uses the following logic:

A minimum of 13 weeks exists between reuse of a cartridge

The cartridge for the 4th week of every month cartridge used is stored off-site

Cartridges from the 4th week of the 1st and 2nd months in a quarter are stored off-site for a 13-week period

Cartridges 4th week of the 3rd months in a quarter are stored off-site for a 2-year period

Off-site storage occurs the 3rd week of the following month

A new cartridge is used for each backup stored off-site for 2 years for the 1st two years. This is cartridge #12 for the 1st 2-year backup and A-G for the next 7 in the cycle.

The following has been designated the “ideal” quarterly cycle for backups using the following logic:

A minimum of a year exists between reuse of a cartridge

Cartridges from the first three backups in a calendar year are stored off-site for a year

Off-site storage occurs the quarter after the backup occurs

A recycled cartridge from off-site is used the quarter after it returns from storage

The last backup of a calendar year is stored off-site for 2 years before recycling

None of the quarterly backups are retained indefinitely

APPENDIX F. BACKUP SOFTWARE

SYMANTEC ADMINISTRATION AND TROUBLESHOOTING

Passwords

Symantec User Accounts

The users in Symantec have accounts whose names may or may not match those of their server login accounts. The passwords for the user logon accounts much match those of the server.

For the purposes of backup, the user for logon to the server and the Symantec software is zsymantec.user. If this user name changes several items must be changed in the Symantec software to continue to use the system. One is the ownership of the selection lists.

On the menu bar pick edit/manage selection lists at which the following dialog box comes up.

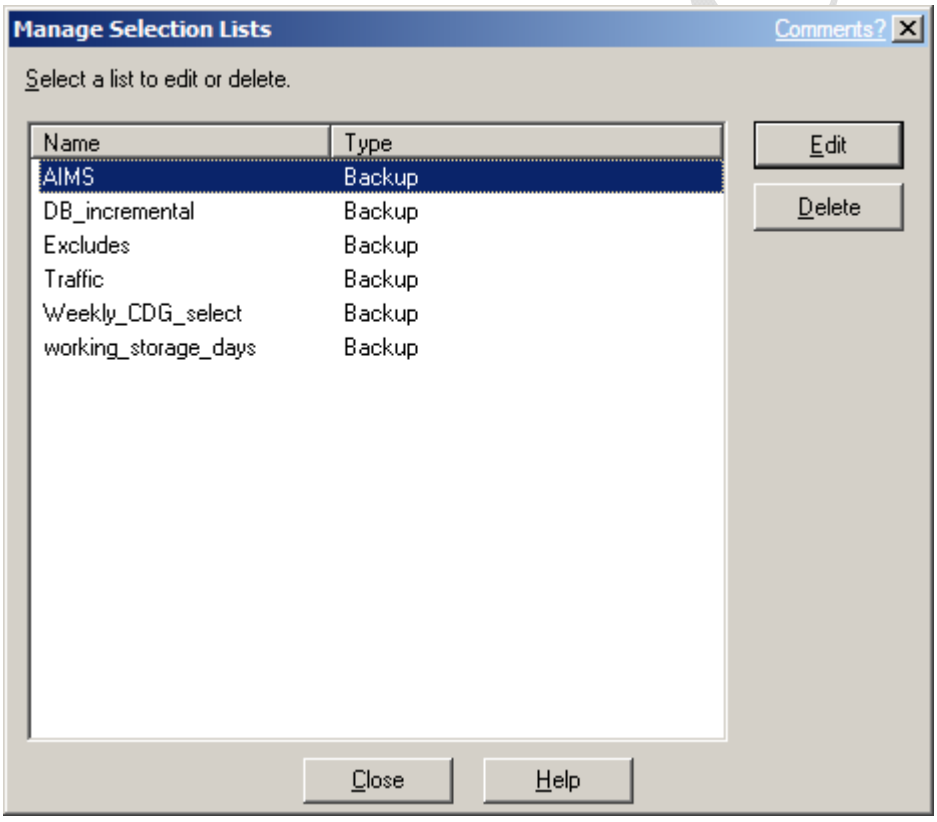


Figure 20. Screenshot. Picking a Selection List to Create a Job

Each list must be checked via edit for a valid logon account.

When edit is selected the following screen will appear

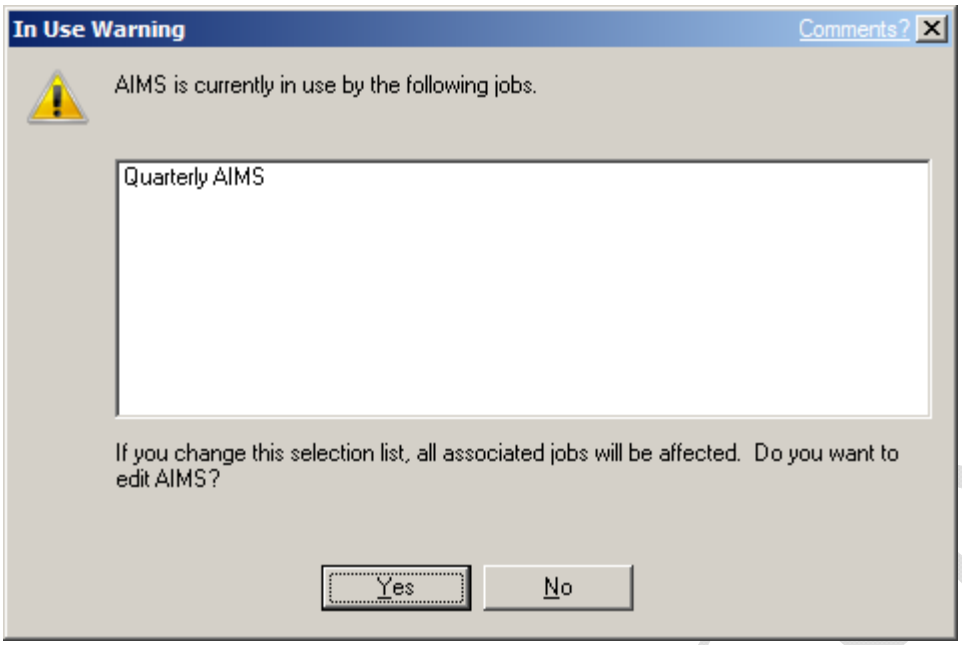


Figure 21. Screenshot. Confirming Changes to a Selection List with Impacts Identified

Click on yes and then

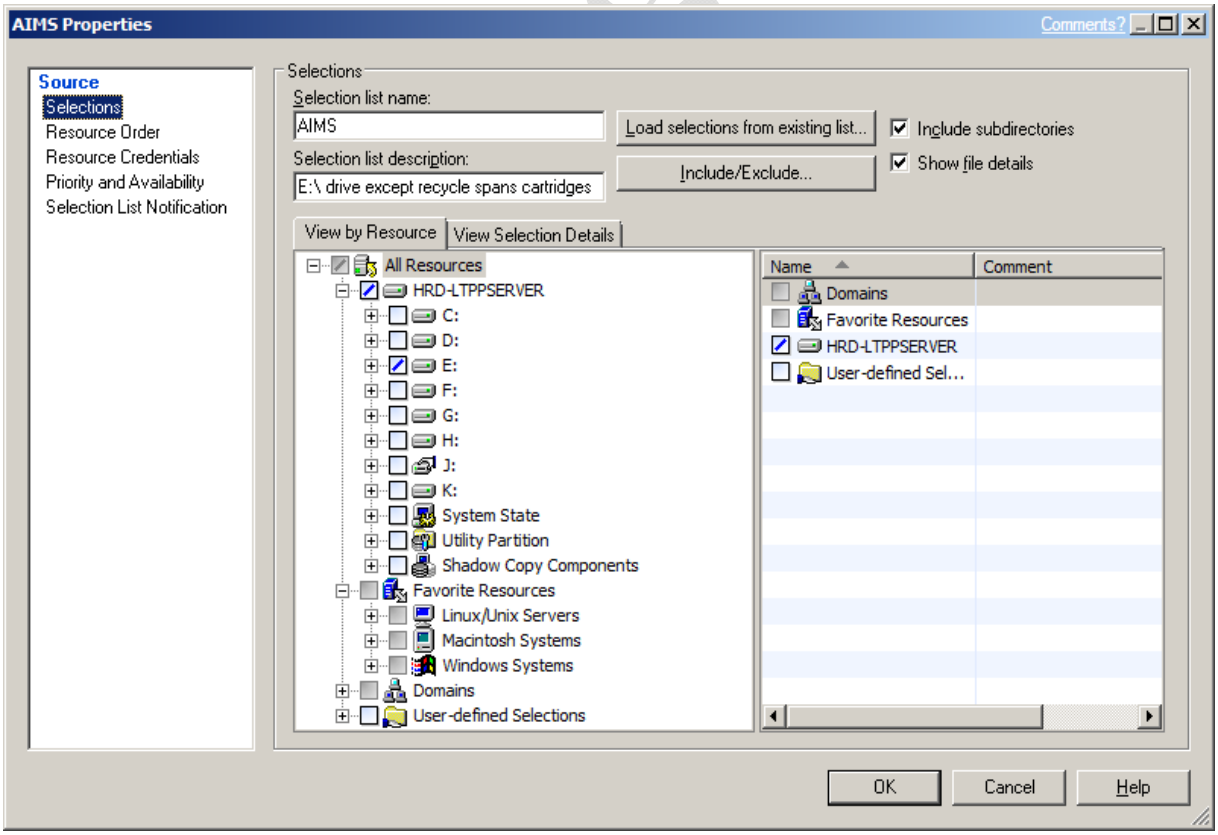


Figure 22. Screenshot. Making Folder and File Selections for Backup

On the following screen click on Resource credentials

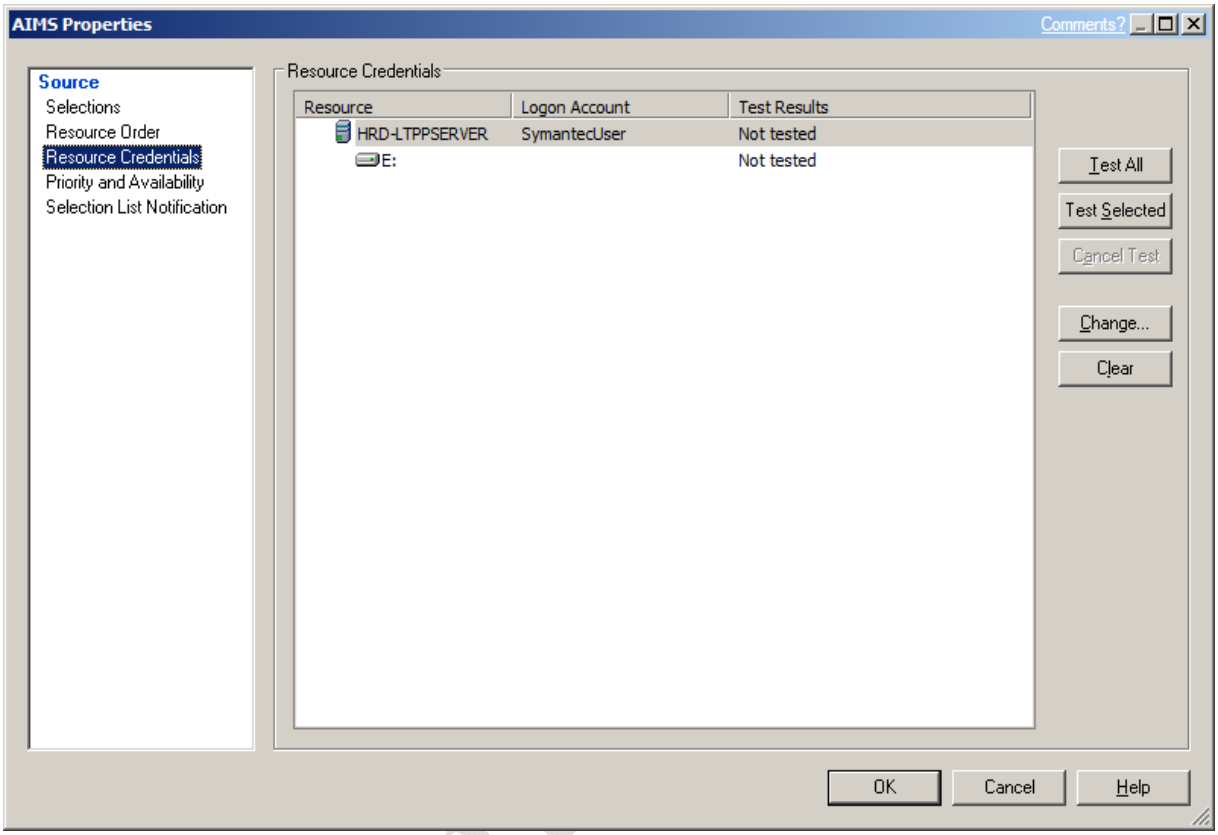


Figure 23. Screenshot. Verifying Access to Drives Identified in Backup Selections

If the logon account does not exist on the server it must be changed using Change.

Change will bring up a list of users. Select the appropriate user and click ok.

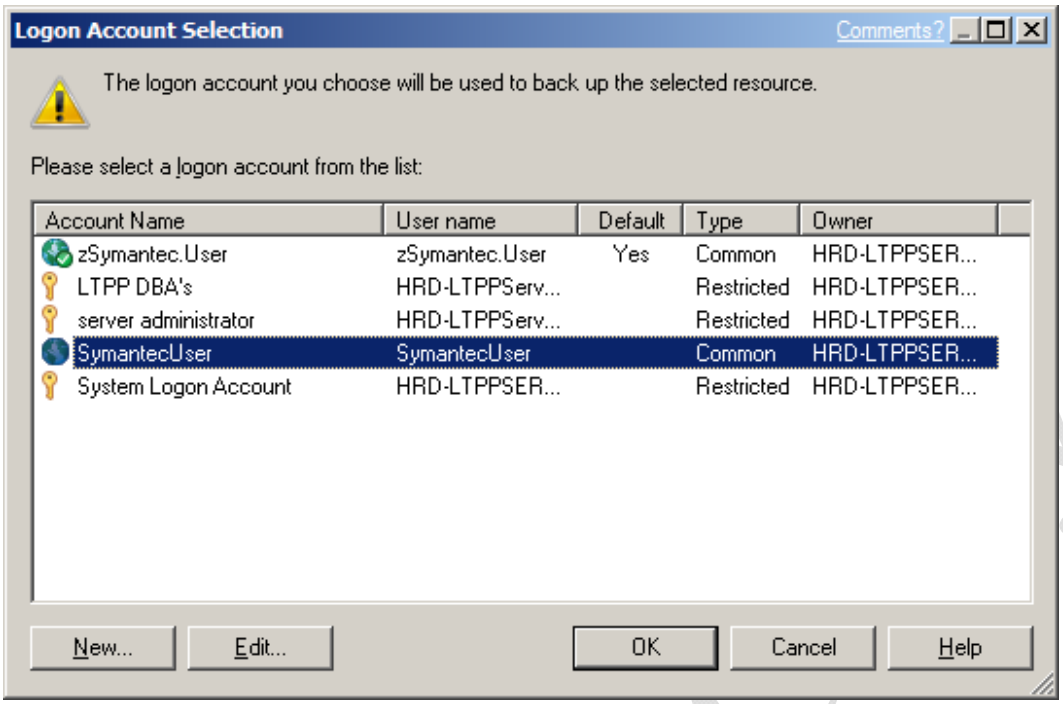


Figure 24. Screenshot. Picking a Logon Account to Run a Backup Job

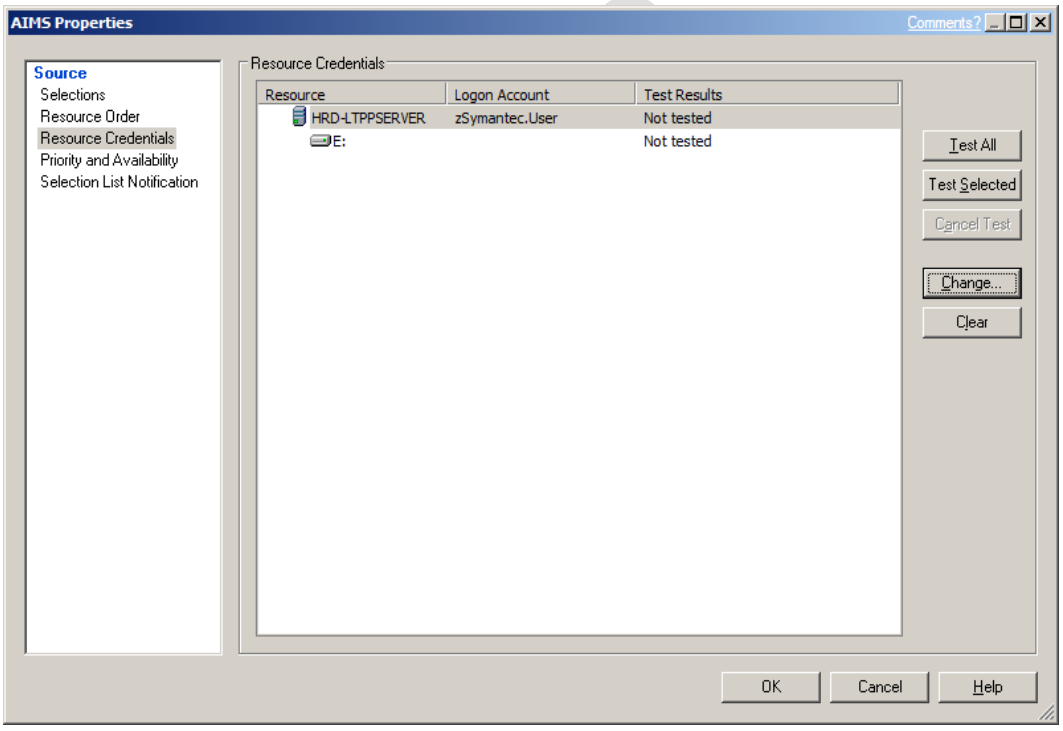


Figure 25. Screenshot. Preparing to Test Access for Backups

Test the Selected or All depending on the number of accounts.

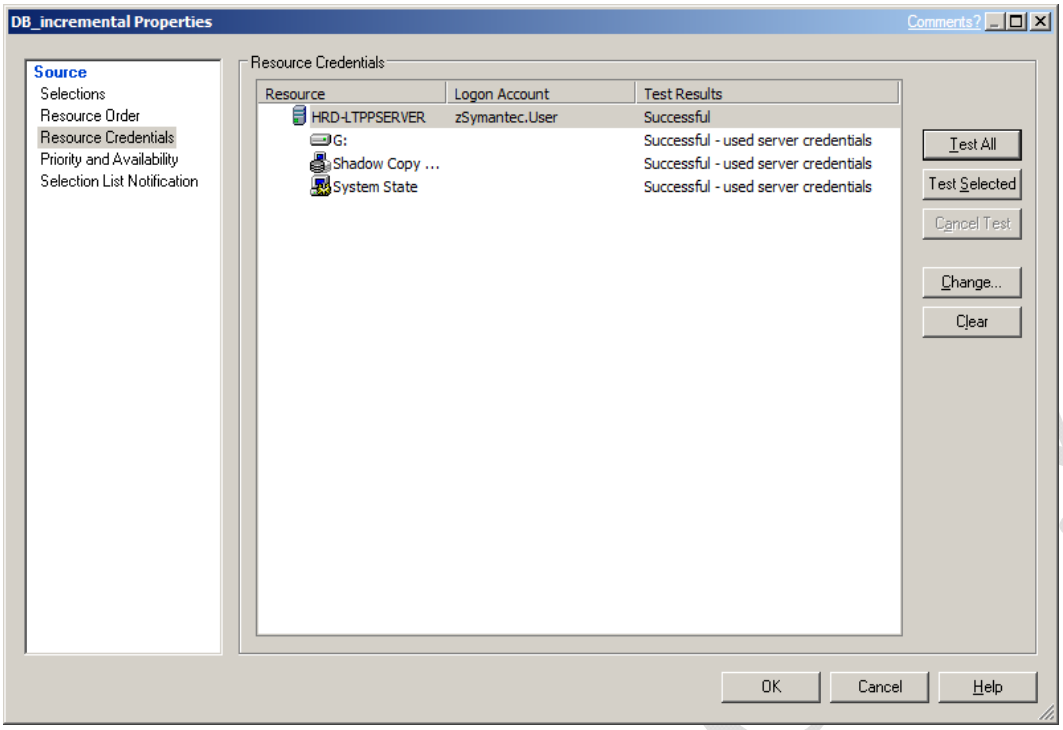


Figure 26. Screenshot. Successful Access Test

A successful test should be accepted by clicking on OK. If it is not successful troubleshoot based on error message displayed.

APPENDIX G. BACKUPS – AN ILLUSTRATED HOW TO

CREATING A JOB

A job is created from the Job Setup screen shown in figure 27. Either the New Job or New job using wizard option from the Backup Tasks box on the left hand side of the screen can be used.

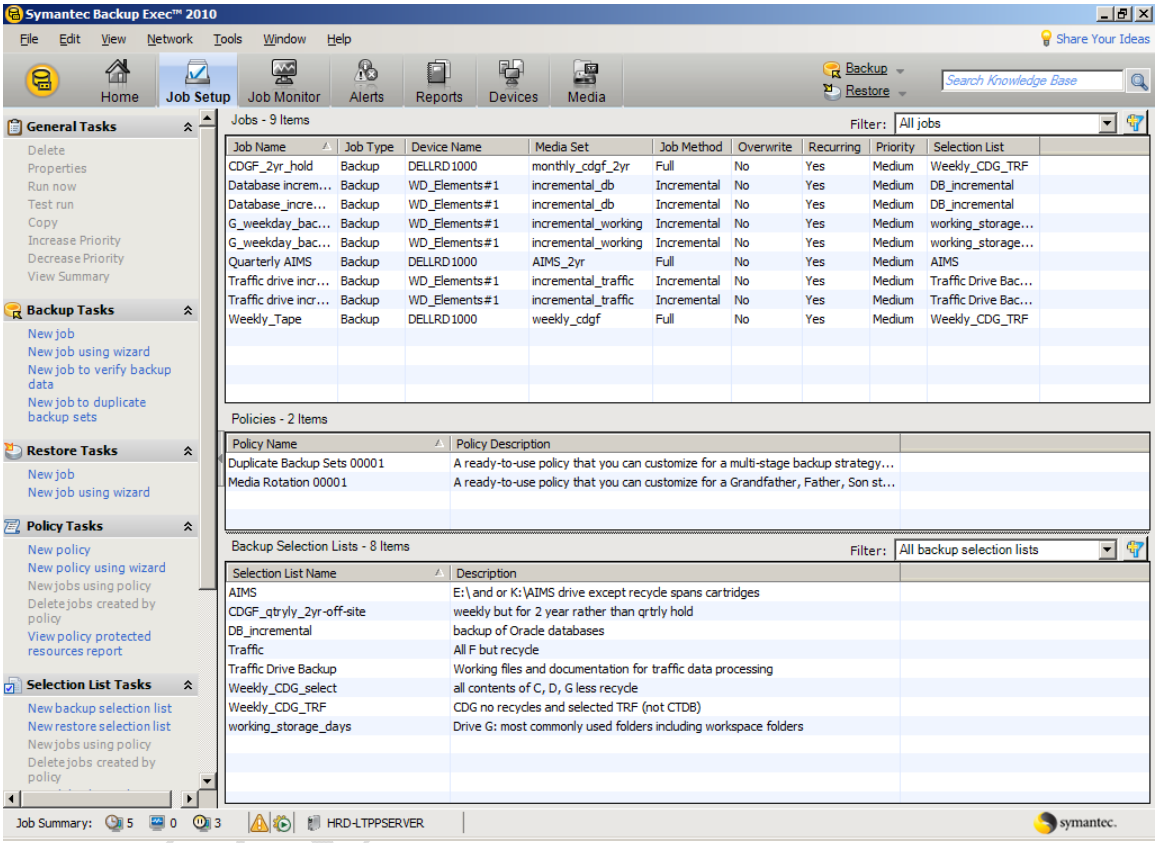


Figure 27. Screenshot. Symantec BE job set up screen.

The upper left box, General Tasks, on the screen has several functions that may be useful: Delete, Properties, Run now, and Test run. Copy is a between server function and not applicable to the LTPP system. These are discussed in Managing jobs.

This discussion goes through the process using the New job option.

Start by clicking on New Job. This will bring up figure 28. The first activity is to select the items to be backed up. If this is the first time this collection of folders/files has been backed up, enter a descriptive name for the list of items under Selection list name to replace the Backup NNNNN naming. Below the name write some text about the materials in the backup.

Do not select show file details unless a by directory listing is absolutely necessary. The list generated in the expanded job log will run to hundreds of pages.

Select the folders and files from each drive.

8. The right hand selection block starting with Domains is not applicable for LTPP.

9. It is recommended to save time and space that the recycle bin not be backed.

10. System state and Shadow Copy Components should generally be included.

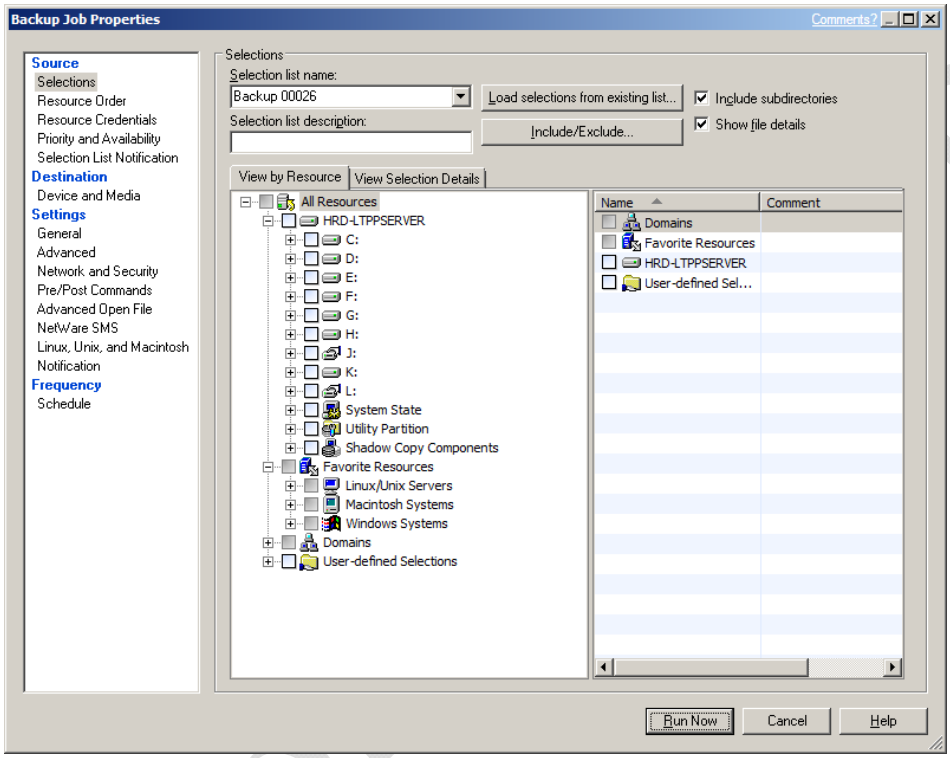


Figure 28. Screenshot. Starting a new job – selections[8].

If this is a copy or variant of an existing backup (incremental version of a full backup for example), click on the arrow beside Backup NNNNN to get a list of existing selection lists (figure 29.) Clicking on the preferred list will populate all the selections as shown in figure 30. The right slash indicates only some of the items are being included. A check mark indicates all items are being included.

[8] Uncheck show file details when making a replacement copy.

If the selection list is going to be a combination of new items and existing lists use the Load selections from existing list option. This will bring up figure 31 or an equivalent list to pick from.

The Include/Exclude option is not currently being used. If the server were having files permanently deleted, or only a specific period was desired in a backup or a differential backup was desired those capabilities can be executed through this selection option.

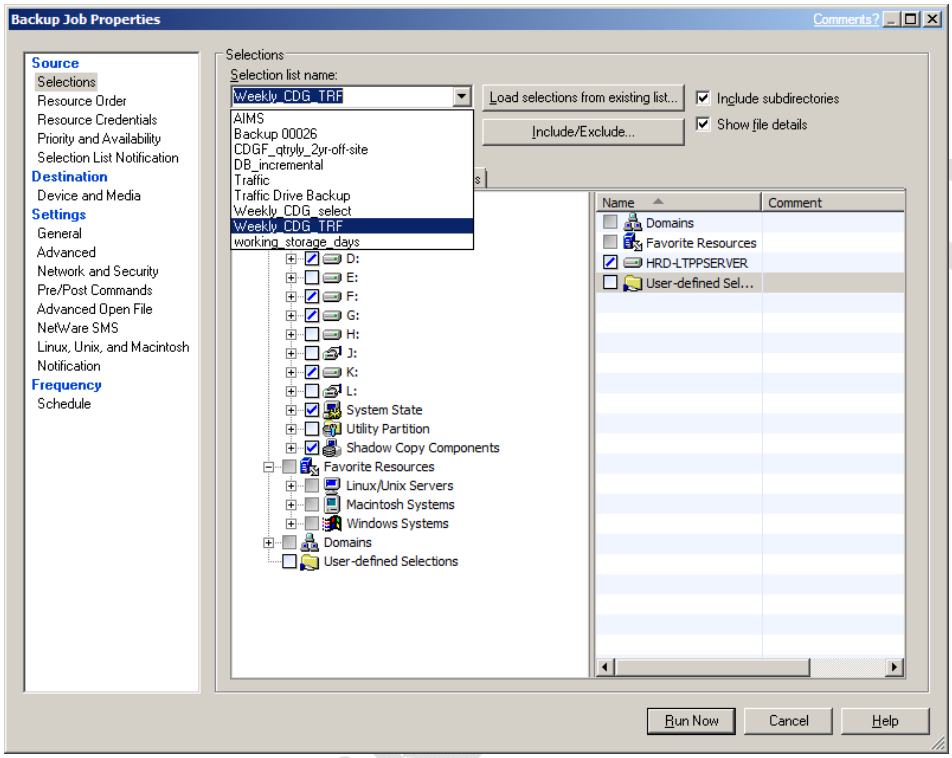


Figure 29. Screenshot. Picking from existing selection lists.

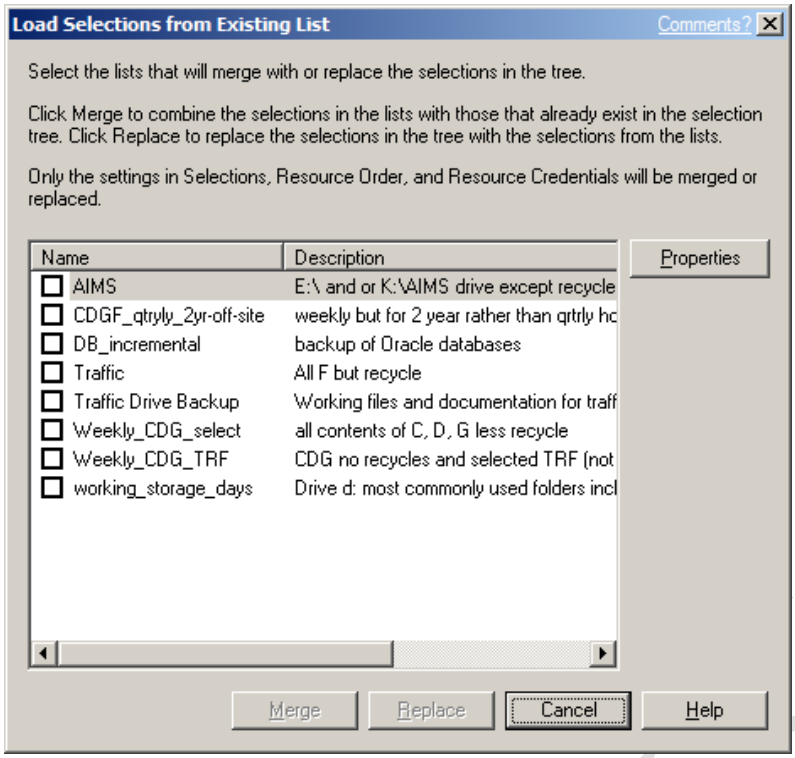


Figure 30. Screenshot. Merge selection options

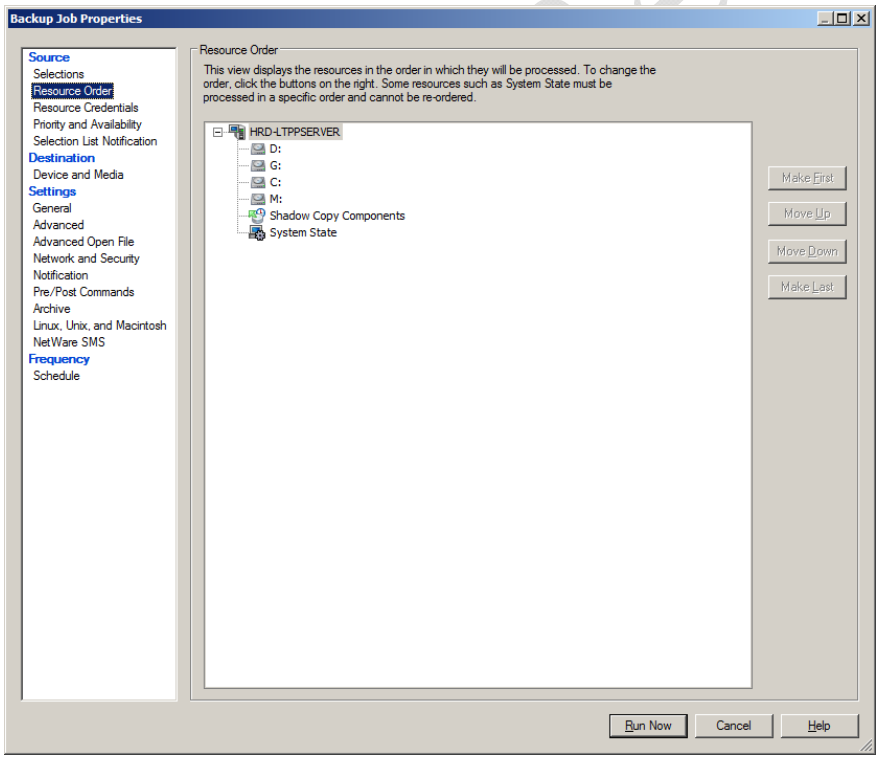


Figure 31. Screenshot. Selecting Resource Order

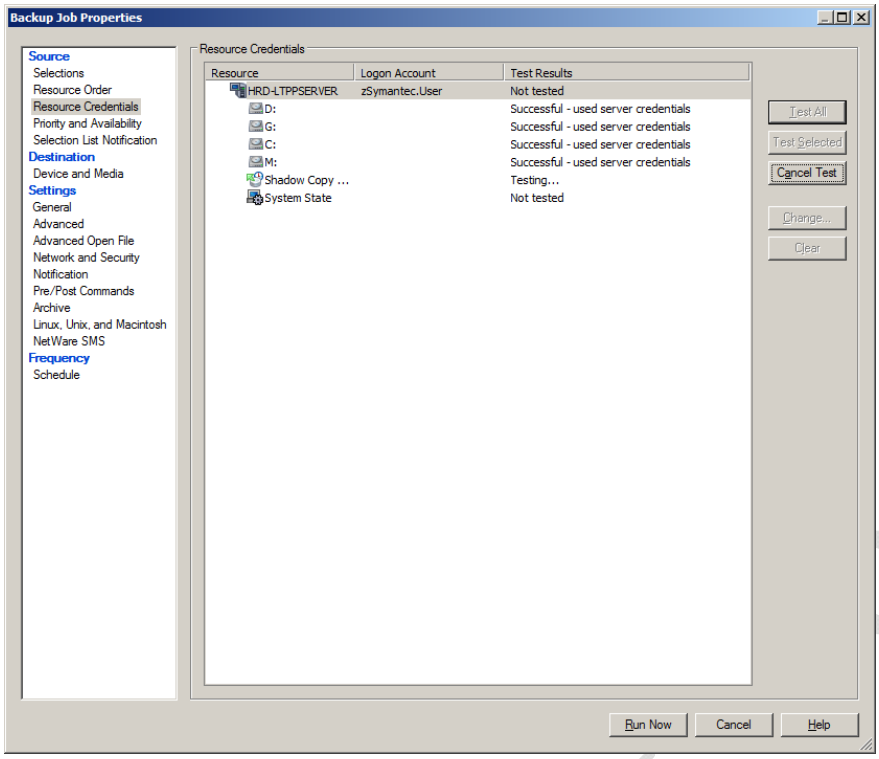


Figure 32. Screenshot. Resource Credential - Testing Log on

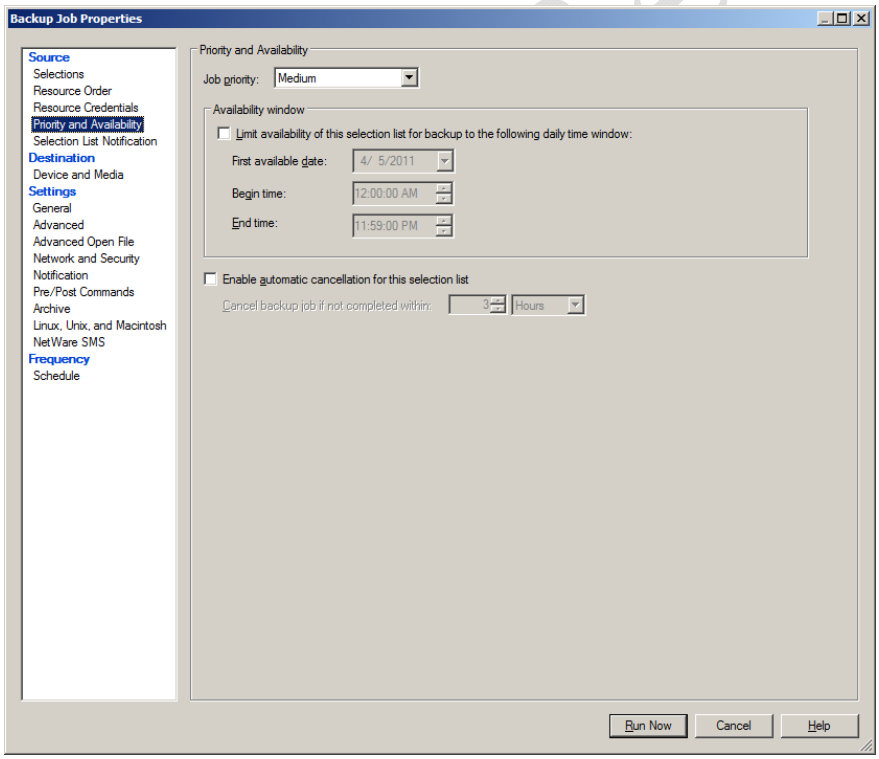


Figure 33. Screenshot. Priority Selection – Defaults

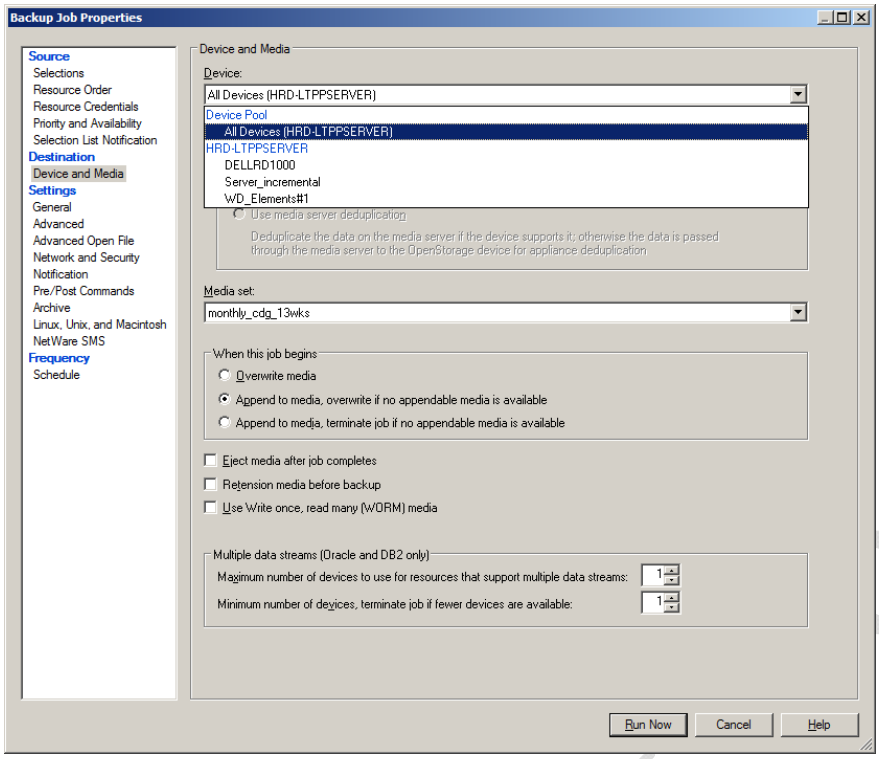


Figure 34. Screenshot. Selecting a Backup Device

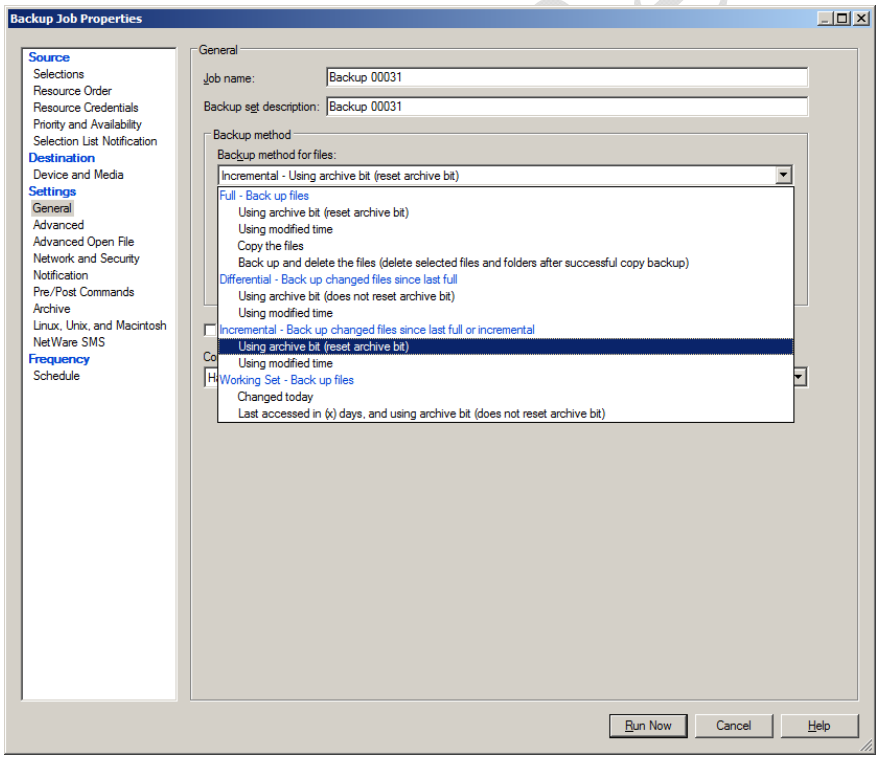


Figure 35. Screenshot. Picking General Settings – Backup Method

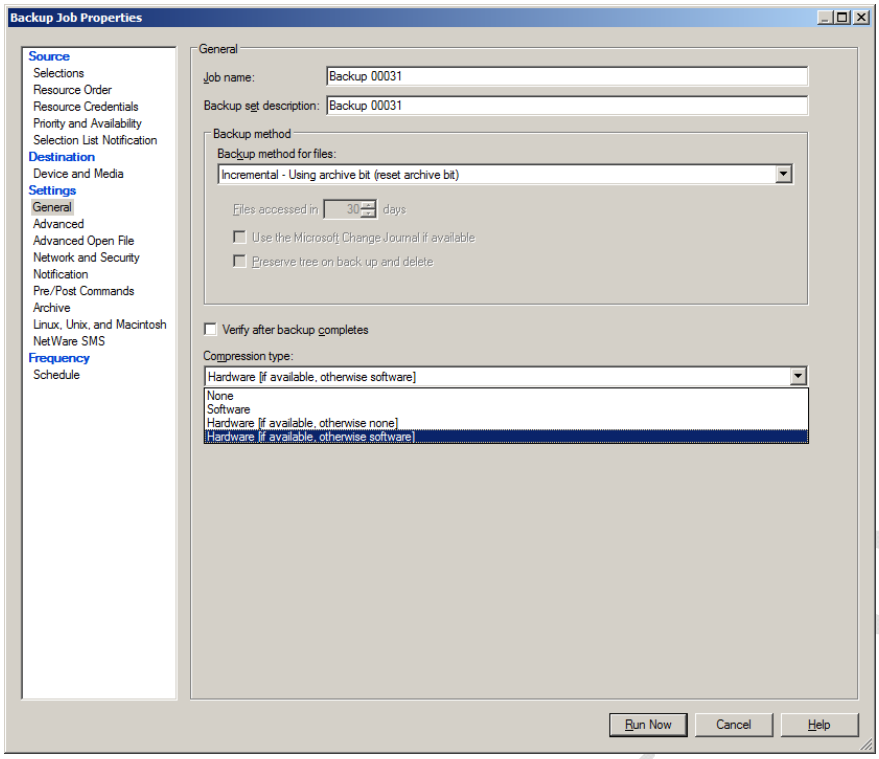


Figure 36. Screenshot. Picking General settings – Compression Type

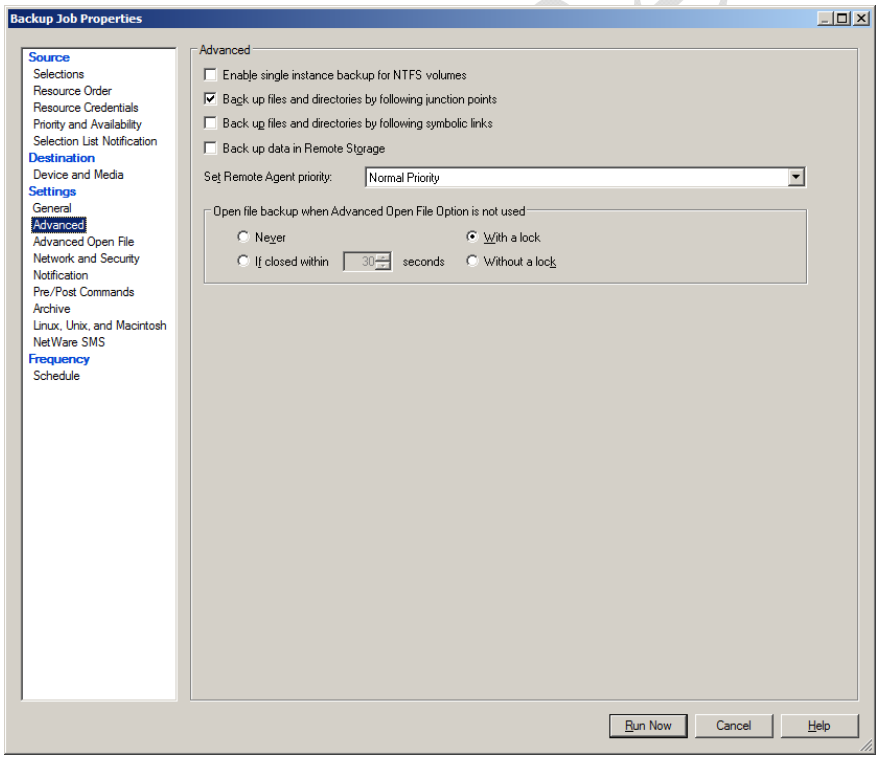


Figure 37. Screenshot. Selection of Advanced Options (Defaults)

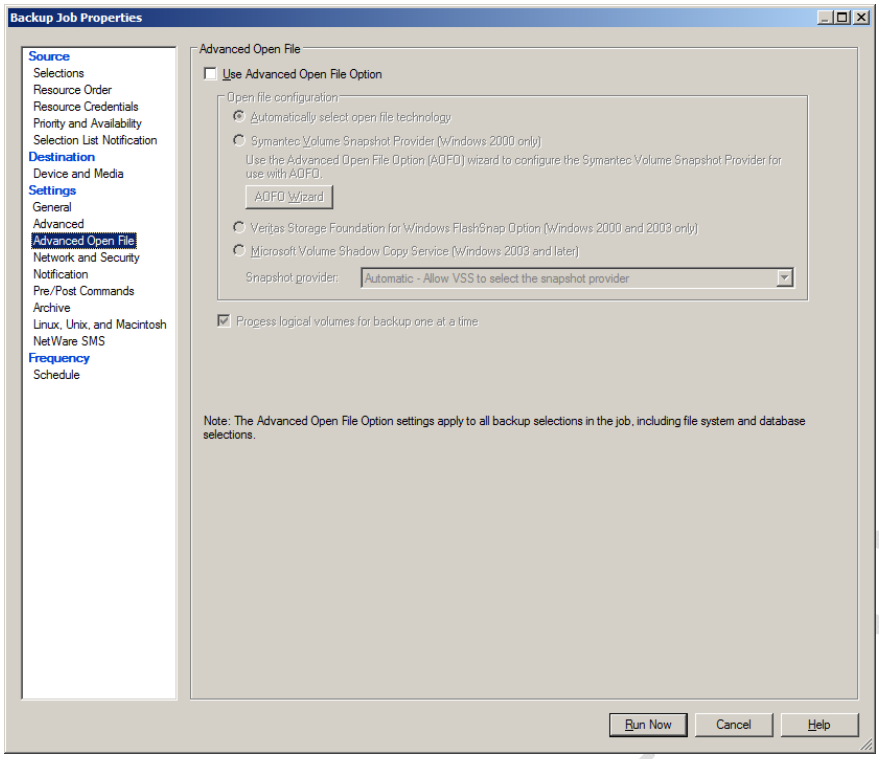


Figure 38. Screenshot. Setting Advanced Open File Options (defaults)

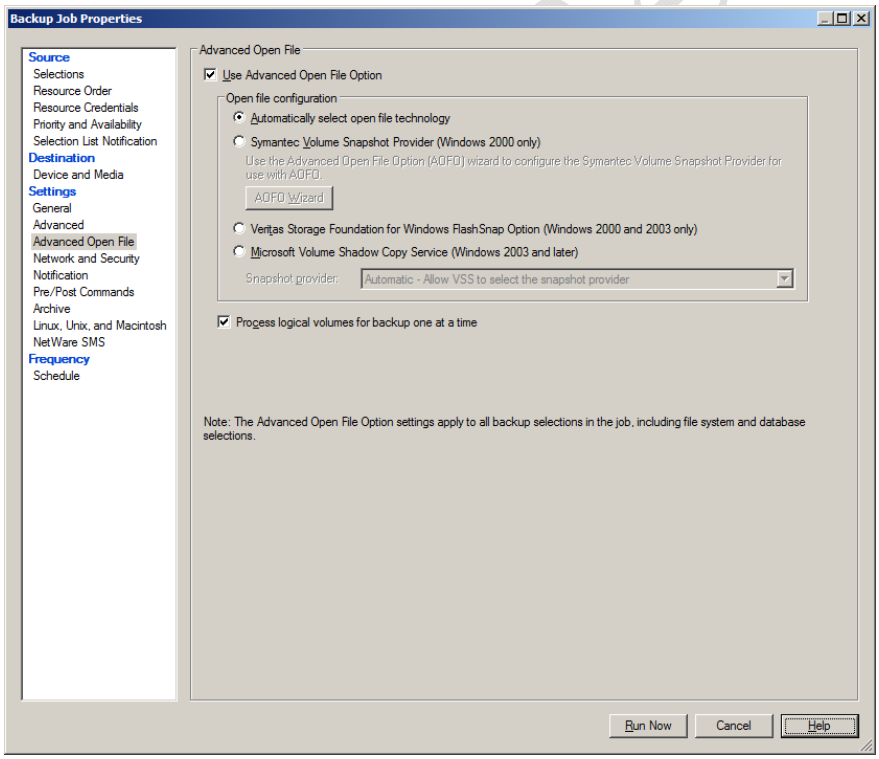


Figure 39. Screenshot. Advanced Open File Options Used

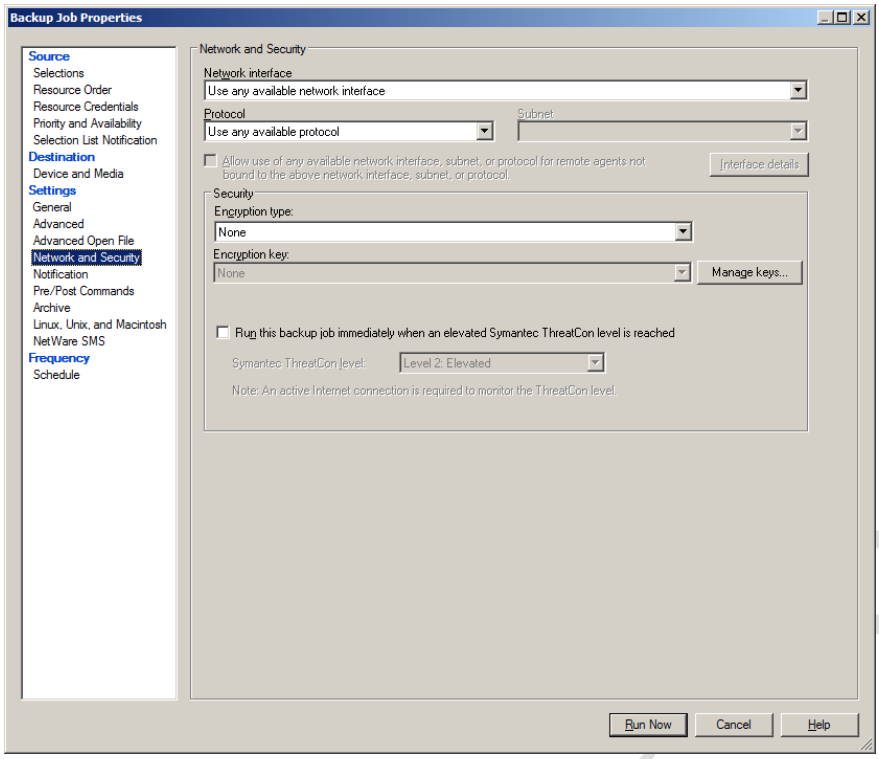


Figure 40. Screenshot. Using Defaults for Network and Security

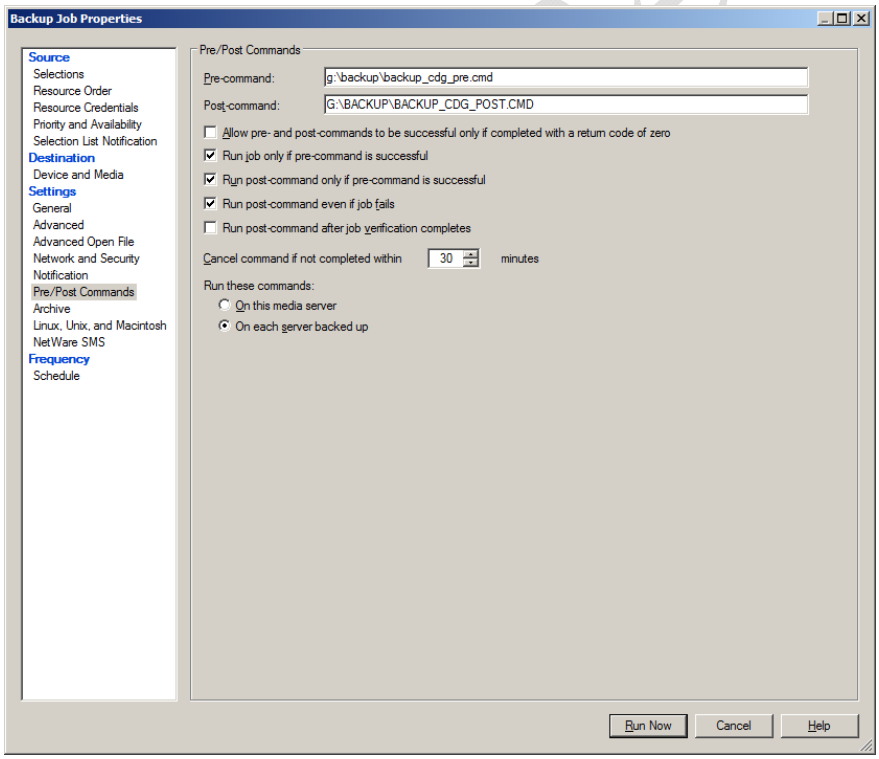


Figure 41. Screenshot. Identifying Pre- and Post- Commands

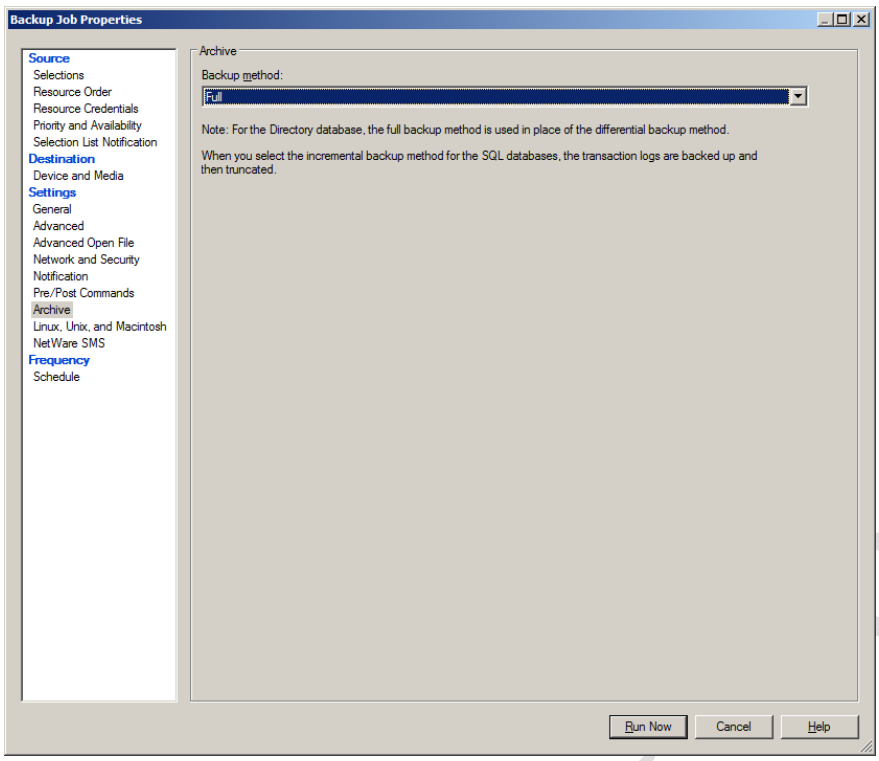


Figure 42. Screenshot. Archive Method Selection

SETTING UP A RECURRING JOB

To set up a recurring job, the same steps of the job set up process as followed with the exception of the schedule selection. *To set various schedule options….*

MANAGING JOBS

The upper left box, General Tasks, on the Job Setup screen has several functions that may be useful: Delete, Properties, Run now, and Test run. Copy is a between server function and not applicable to the LTPP system.

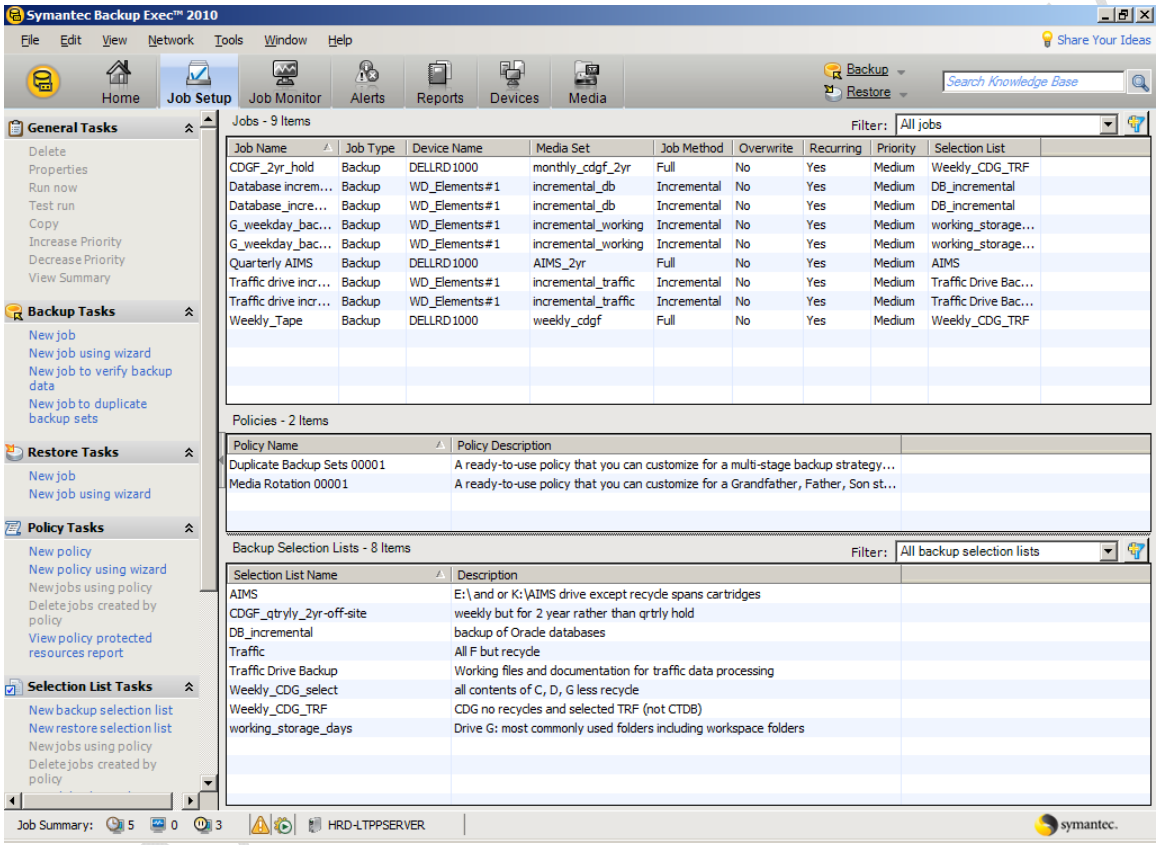


Figure 43. Screenshot. Job functions accessible through Job Setup screen.

Delete does exactly what it says, removes a job from the list. Highlight a job and click on it. The response will be the dialog box in figure 44. The selection list option exists to remove the information about what is being backed up. Unless the list is used only for the job or is not anticipated to be used in the future, it should not be deleted.

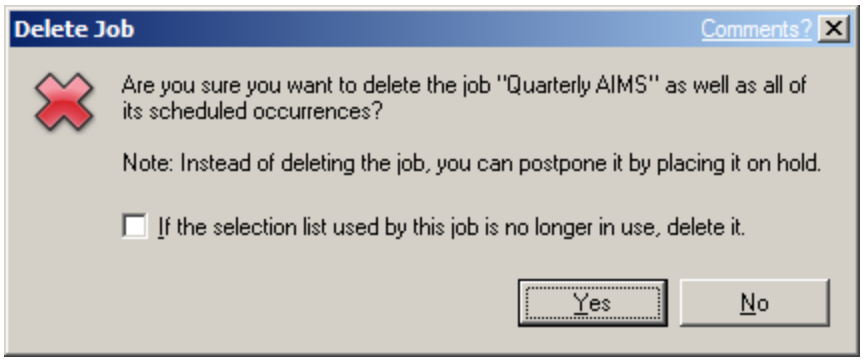


Figure 44. Screenshot. Delete Confirmation dialog box

Selection of a job and clicking on Properties provides the capabilities to edit an existing job. The dialog box in Figure 45 will appear after the selection and click. Any item on the list may be checked and changed if necessary. To save any changes click on "Submit". The revised properties should be saved for reference by creating a pdf in the associated backup log folder.

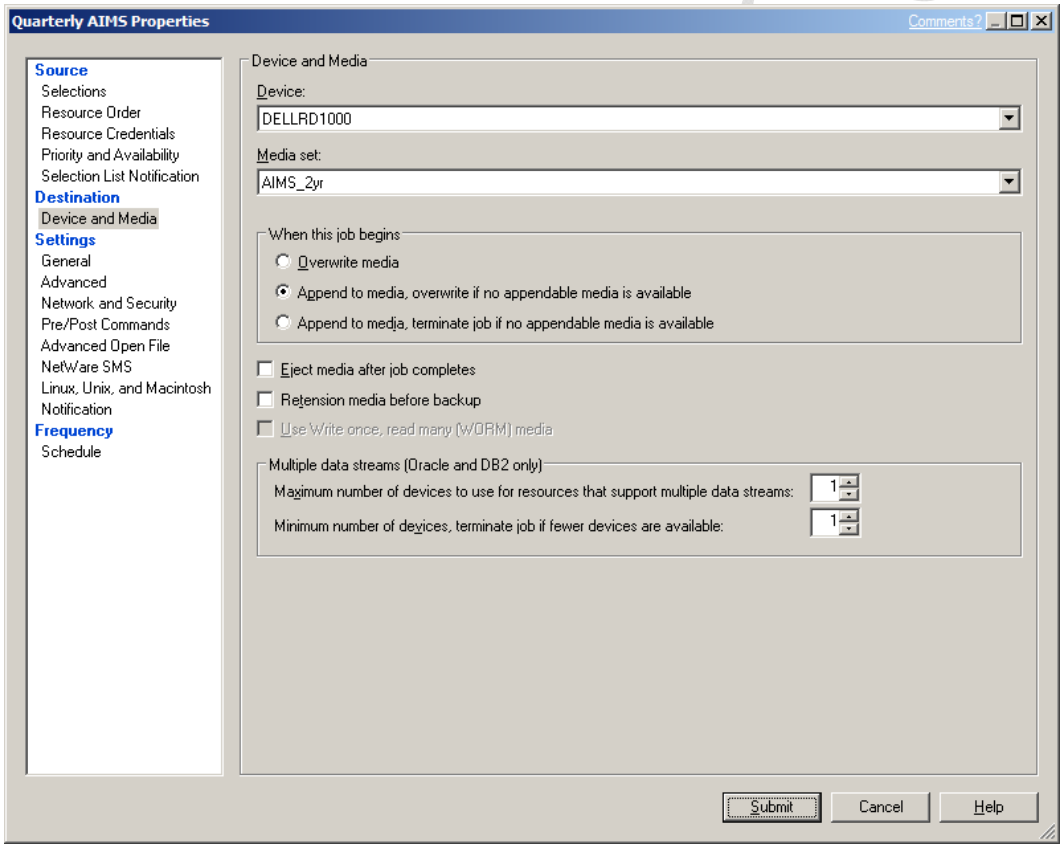


Figure 45. Screenshot. Initial Properties dialog box.

The Test run function checks that all of the pieces are present, drives accessible to the user, command files for pre and post job actions readable and so forth. It will execute all of the elements of the backup job except the actual backup.

The Run now option starts a job immediately rather than waiting for a scheduled time or setting up a schedule.

REVIEWING JOB HISTORY

SAVING BACKUP REPORTS

Printed copies of backup reports are created once a week to have a “permanent” record of backups made and their content. Printed copies are made with Adobe Acrobat.

Job reports can be stored indefinitely in BE. These guidelines have been established to set limits on the amount of information stored.

Figure 46 shows a series of folders on drive F:\Working Storage of the server that apply to backups. Included are the folders Backup_logs and IDR.

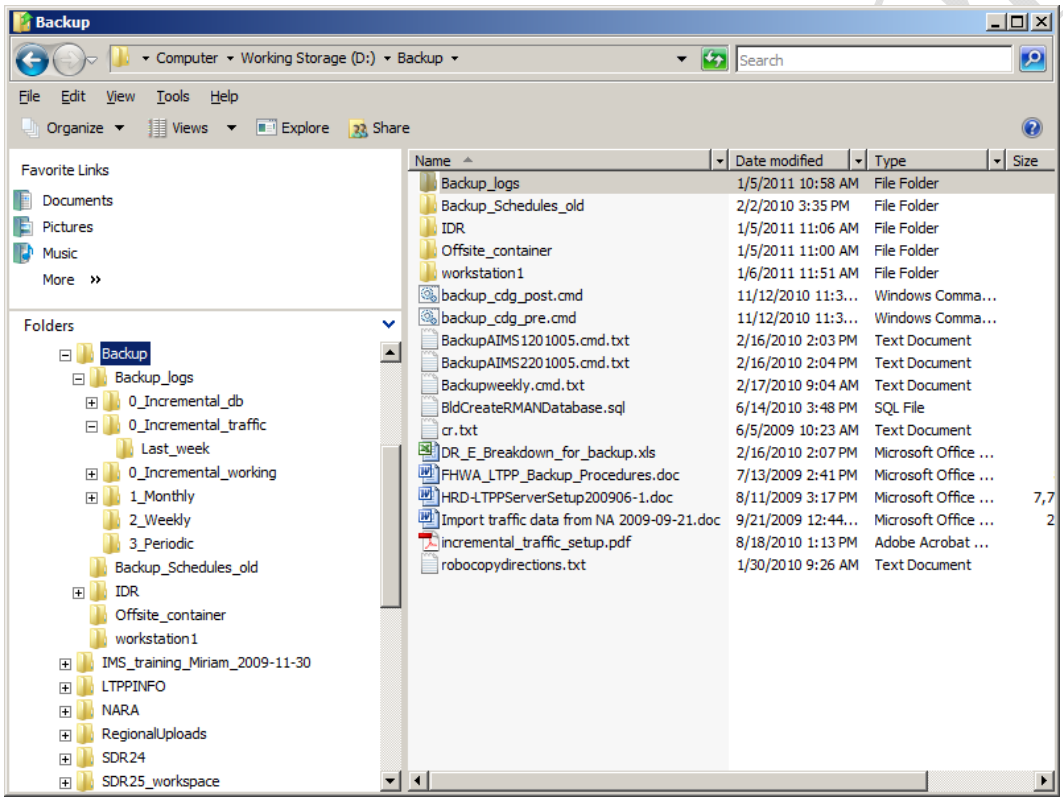


Figure 46. Screenshot. Folders on server for storing backup reports.

The folder Backup has three sub folders: Backup_logs, IDR and Offsite_container. IDR (Intelligent Disaster Recovery) is a folder used by BE. Offsite_container contains files on the original system for storing cartridges off-site. It will be removed January 2011 after all cartridges have cycled into the new backup and container schedules. Backup_logs holds all the copies of the backup job set ups, histories and logs.

There are six sub-folders under Backup_logs: 0_Incremental_db, 0_Incremental_traffic, 0_Incremental_working, 1_Monthly, 2_SDR, 3_Weekly, 3_Periodic.

- 0_Incremental_db – incremental backup of the LTPP Oracle databases (G:)
- 0_Incremental traffic – incremental backup of the traffic drive (F:)
- 0_Incremental_working – incremental backup of the working storage drive (D:)
- 1_Monthly – full backups that are stored off-site for either 13 weeks or 2 years
- 2_SDR – backups of the most recent SDR instance.
- 3_Weekly – full backups that are retained on site.
- 3_Periodic – Quarterly backups.

A folder contains three types of pdfs: job setups, job histories and job logs. Job setups are the final step of the process in creating a job. The 0_* folders have a Last_week subfolder to store prior weeks pdfs.

Job histories and Job logs are created as follows:

Select the Job Monitor tab

Select a job in the Job History section

Right click on the job to bring up the menu box as shown in Figure 47. Select the earliest if multiple jobs of the same type have run.

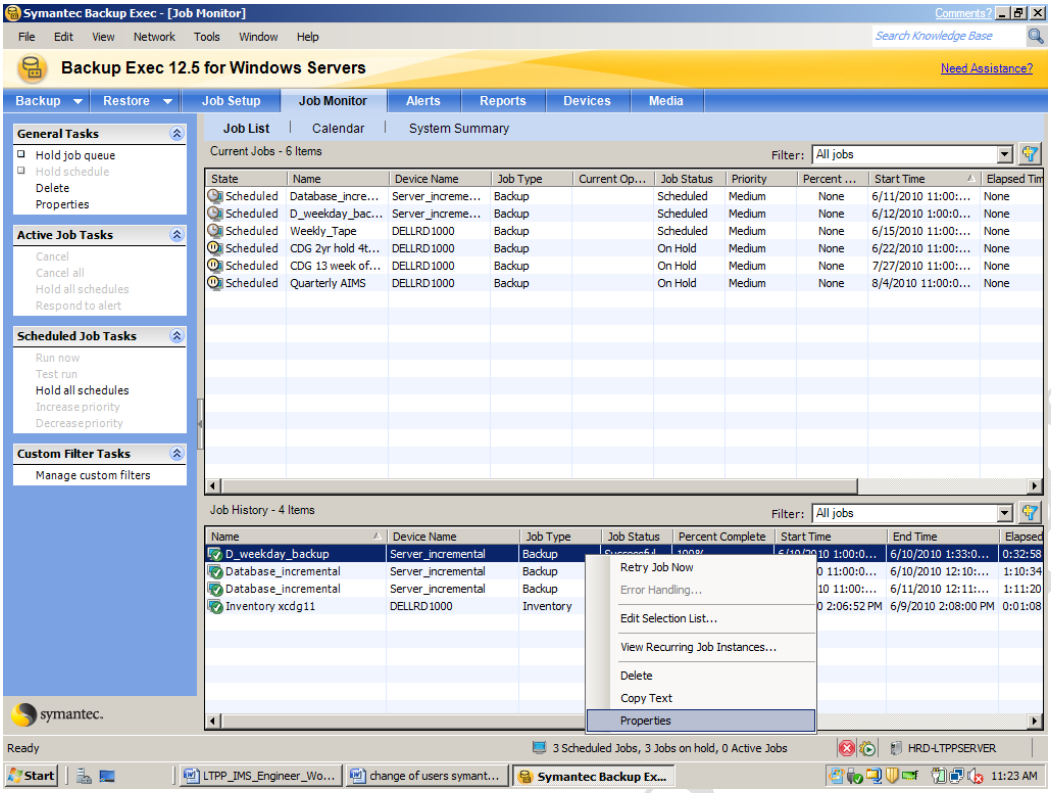


Figure 47. Screenshot. Selecting a Job to Print

Click on Properties.

The Properties selection brings up the Job history screen with its two tabs: Job History and Job Log. Click on Job History The condensed version comes up as shown in Figure 48.

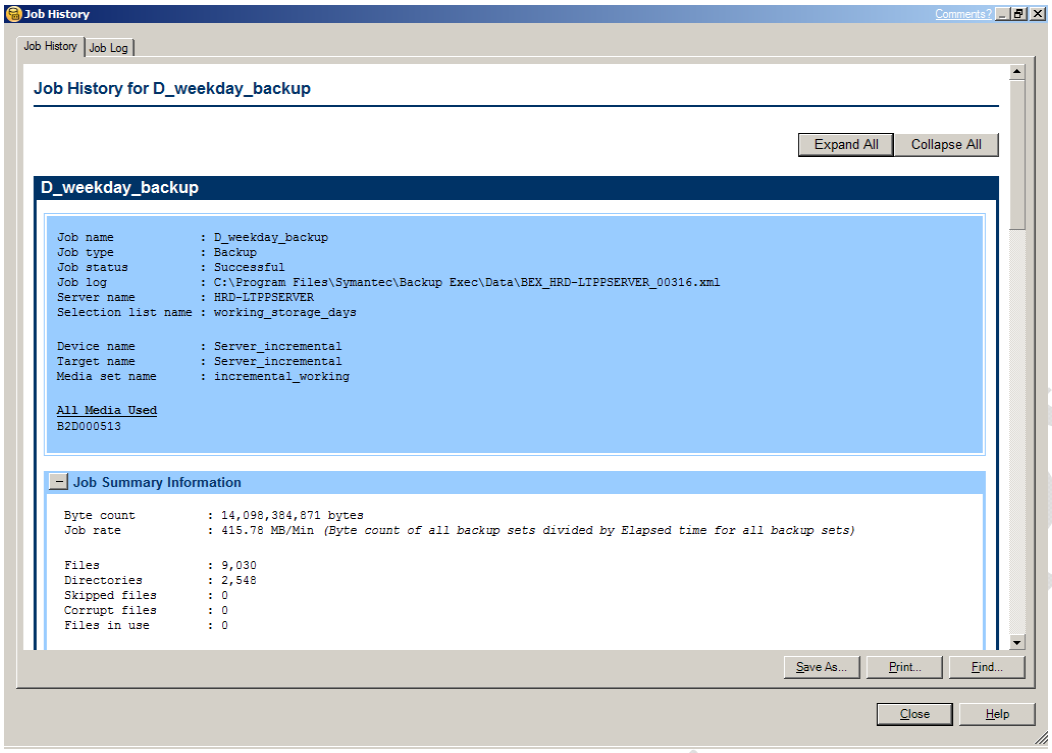


Figure 48. Screenshot. Job History screen

Click on Job History to ensure it is in front

Click on Expand All (upper right corner)

Click on Print (lower right corner.)

The printer selection menu will come up (Figure 49). Adobe PDF should be the default printer. If not, select it and then click on Print. The filename that comes up is that assigned by BE (Figure 50).

Before changing the file name, verify that the correct directory (Figure 46) in G:\Backup\Backup_logs has been selected.

Enter the file name.

Using the file naming convention, type the first letter of the file name. It can be simpler to edit an existing file name than to type one from scratch. The file name in this case where the Job History tab is forward will be the ‘hist’ version. The dates in the files are the date the backup being printed was STARTED, not the date it finished. If the backup failed, a printout is still made to know which backups do and do not exist. The History or the Log may be missing depending on the type of failure.

The file naming conventions for the various folders are as follows:

- 0_Incremental_weekday – I_work_hist/log_yyyymmdd(_fail)
- 0_Incremental_db – I_db_hist/log_yyyymmdd(_fail)
- 0_Incremental_traffic – I_traffic_hist/log_yyyyymmdd(_fail)
- 1_Monthly – cdgfNN_hist/log_yyyymmdd(_fail)
- 2_SDR_>>>>>
- 3_Weekly – cdgfNN_hist/log_yyyymmdd(_fail)
- 3_Periodic – AIMS_tape#_mmyyyy

Click on Save.

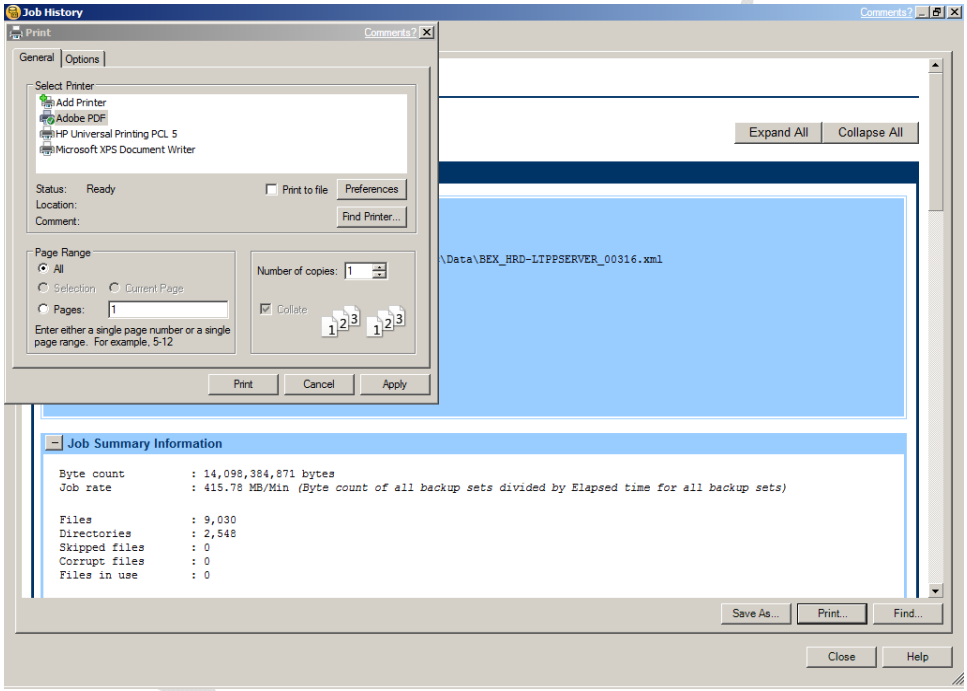


Figure 49. Screenshot. Selecting a printer.

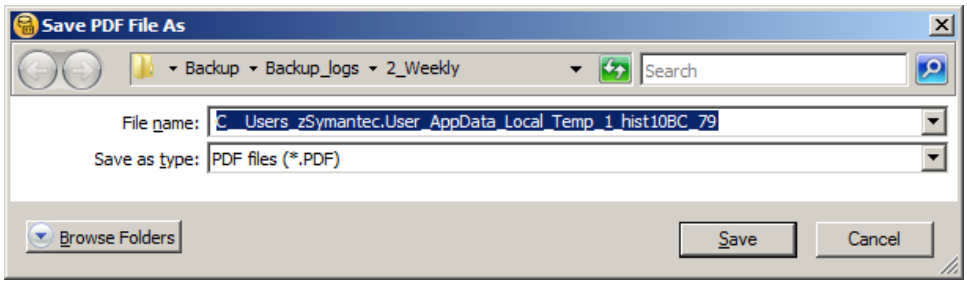


Figure 50. Screenshot. Locations and names for job logs.

Verify the full (expanded) history was printed when it comes up in Acrobat.

Click on Job Log to ensure it is in front (Figure 51).

Click on Expand All (upper right corner)

Click on Print (lower right corner.)

The printer selection menu will come up (Figure 49). Adobe PDF should be the default printer. If not, select it and then click on Print. The filename that comes up is that assigned by BE (Figure 50).

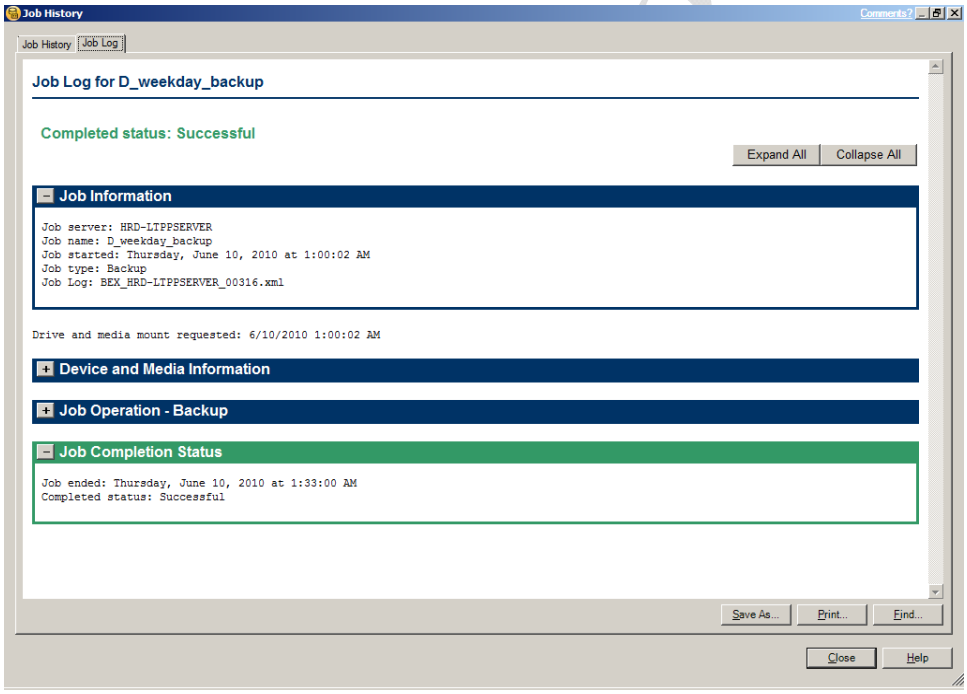


Figure 51. Screenshot. Job Log screen - Summary Form.

Enter the file name.

Type the first letter of the file name. The file name in this case where the Job Log tab is forward will be the ‘log’ version. The dates in the files are the date the backup being printed was STARTED, not the date it finished. If the backup failed, a printout is still made to know which backups do and do not exist. The History or the Log may be missing depending on the type of failure.

Click on Save.

Verify the full (expanded) log was printed when it comes up in Acrobat.

Click on Close.

Return to Symantec and the next Job to be printed.

When all jobs have been printed delete them from the Job History section of Job Monitor.

Add notes on tape replacement; printouts which may not occur

File management discussion: saving; length to hold; length to recycle.

PREPARING FOR RECOVERY

On at least a monthly basis after an off-site tape is created a copy of both the disaster recovery file and a bootable image of the primary drive should be updated. The former is referred to as a .dr file in Symantec BE terms. The latter is referenced as an .iso file, an image to be copied to DVD in order to be used. The creation of both items is done through the Intelligent Disaster Recovery Preparation Wizard.

Select Prepare for (Intelligent) Disaster Recovery in the Job Setup screen once to prepare the .iso file and a second time to create the .dr file.

There may be a User Account control to validate continuing. If so, Click on Continue.

The Wizard will come up. The IDR option has been installed on the server so the block on the screen can remain unchecked before clicking on Next

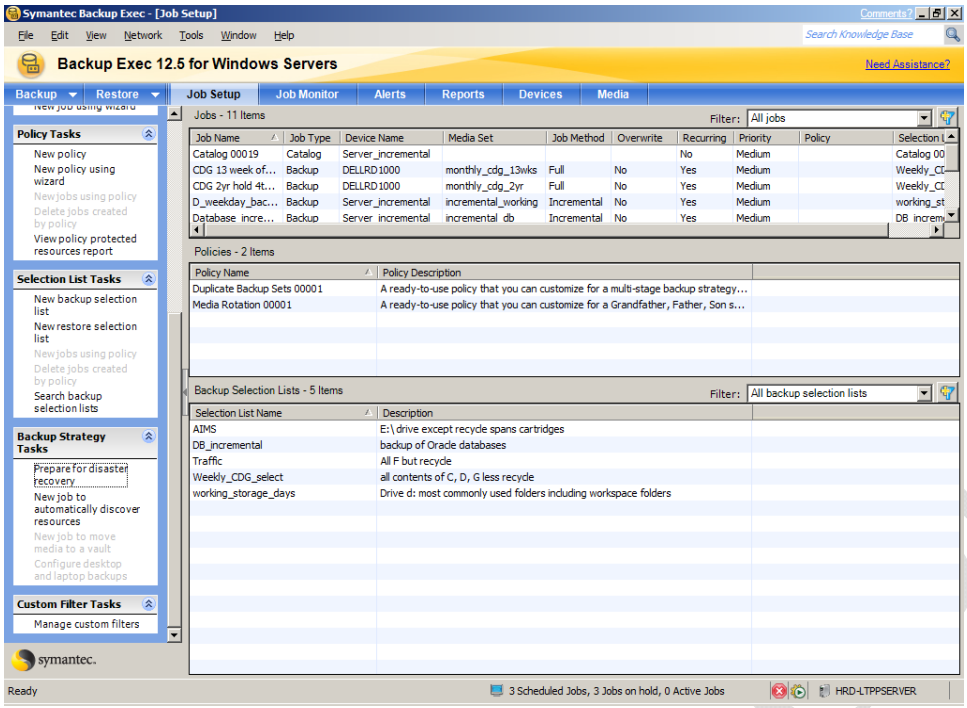


Figure 52. Screenshot. IDR Wizard - replace 2010

Figure 53. Screenshot. IDR Preparation Wizard Opening Screen

IDR Preparation

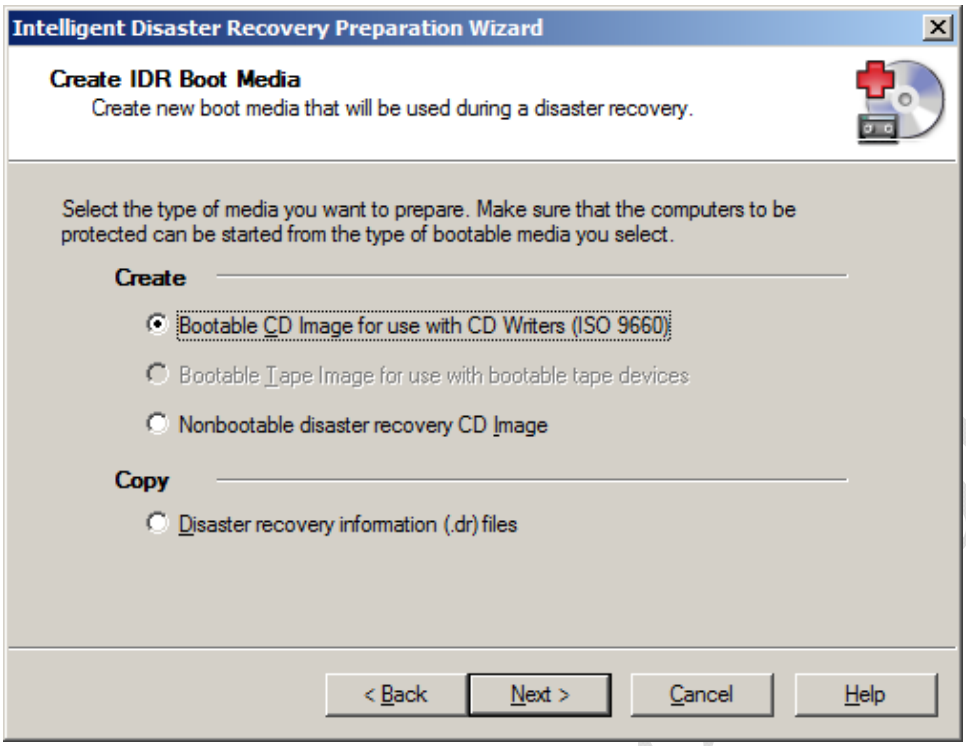


Figure 54. Screenshot. IDR Boot Media Options

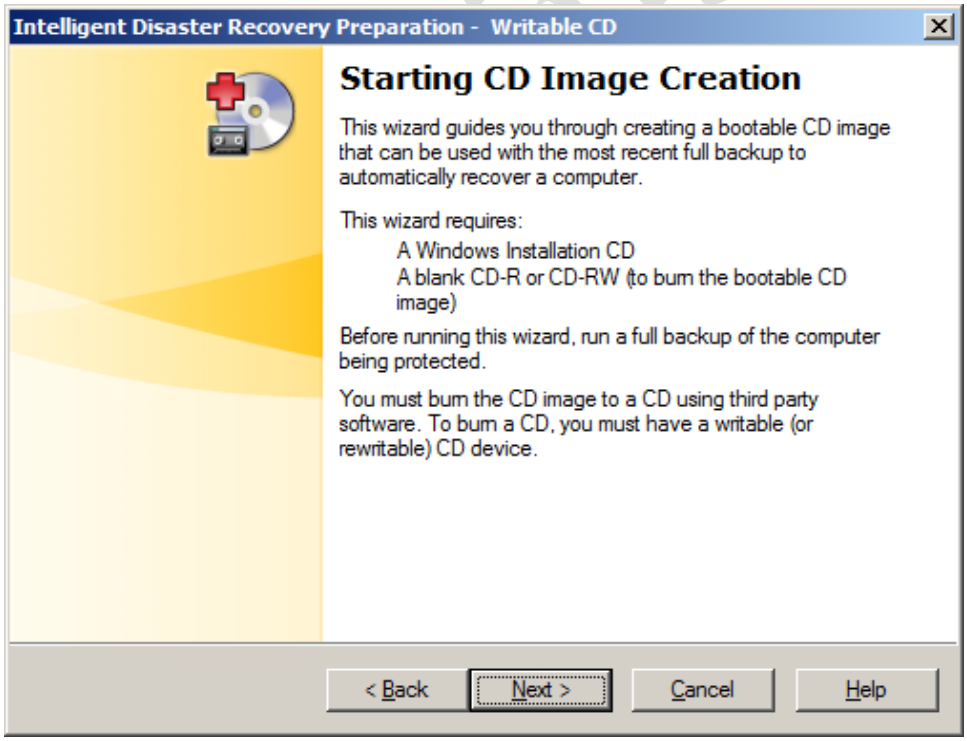


Figure 55. Screenshot. IDR CD Creation Instructions

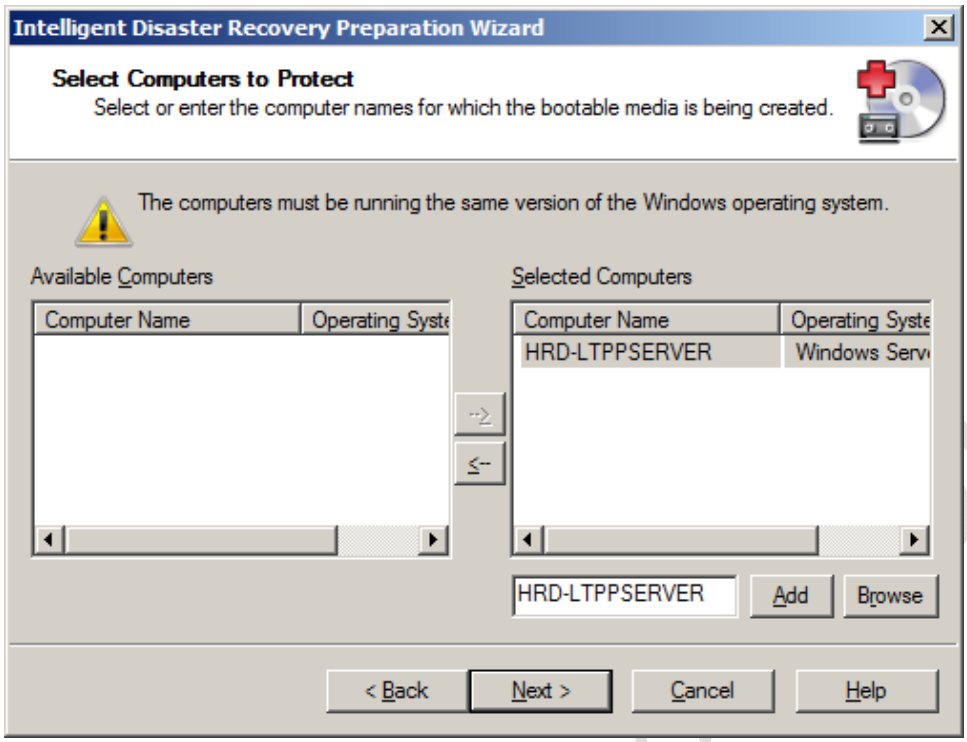


Figure 56. Screenshot. Selecting a Computer for Disaster Recovery Preparation – Replace – new server name

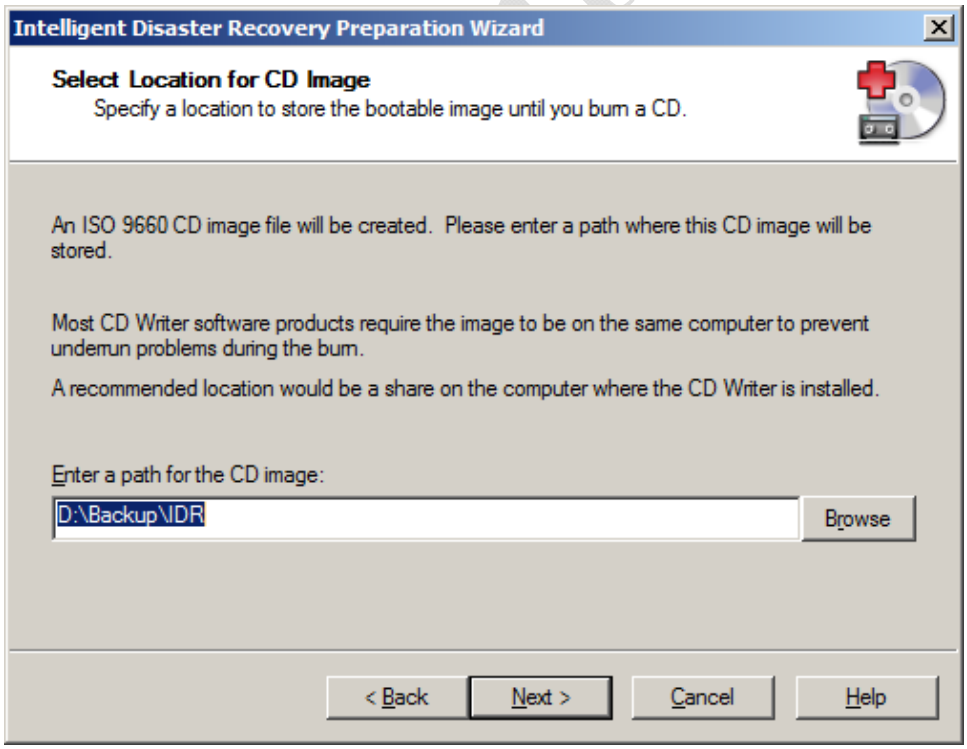


Figure 57. Screenshot. Location Selection for CD Image

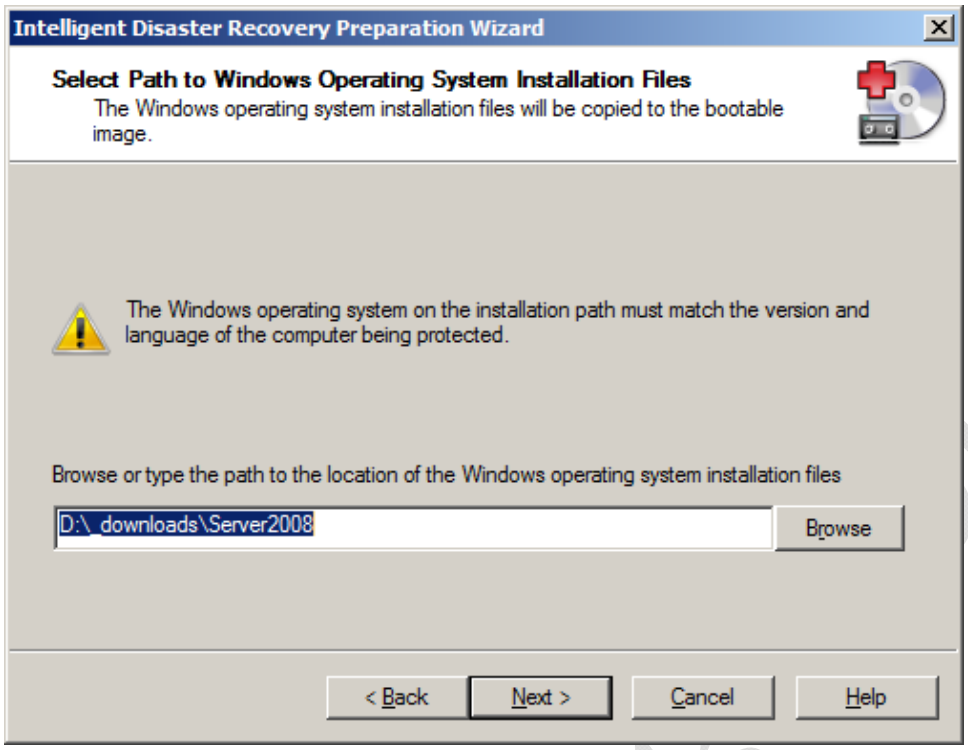


Figure 58. Screenshot. Identifying Windows OS Installation File Location

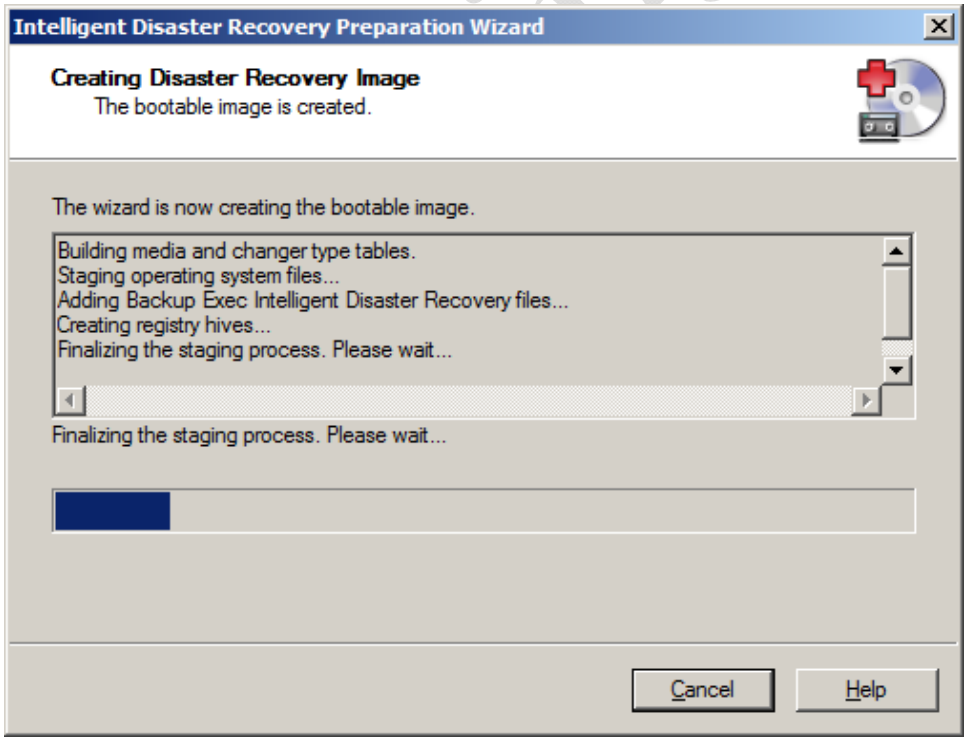


Figure 59. Screenshot. Image Creation Messages

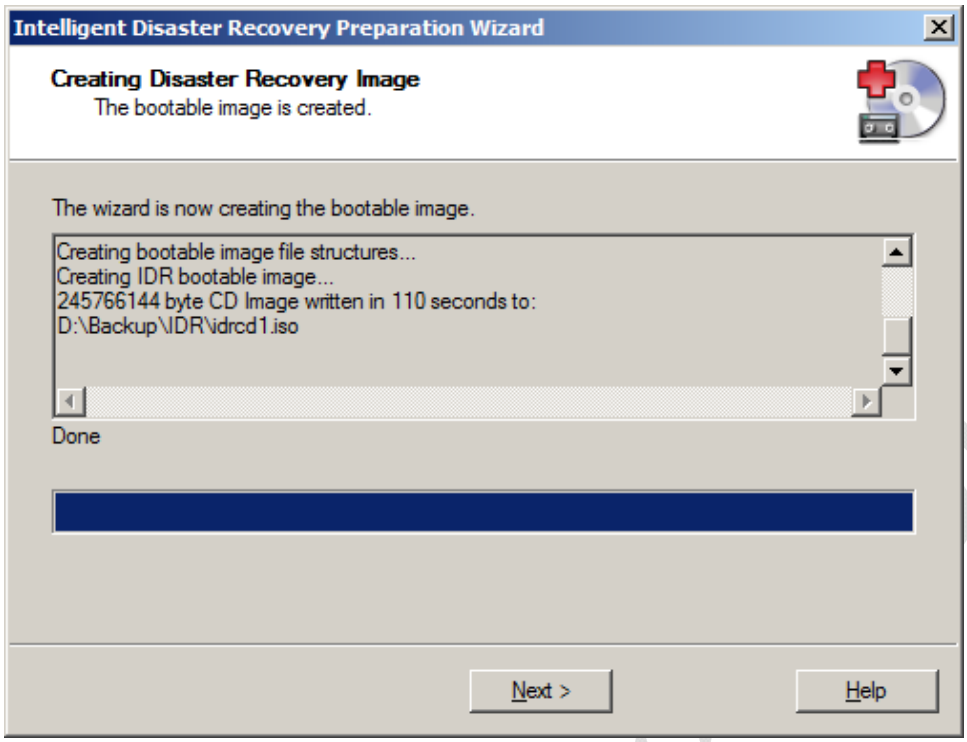


Figure 60. Screenshot. Outcome of Disaster Recovery Preparation

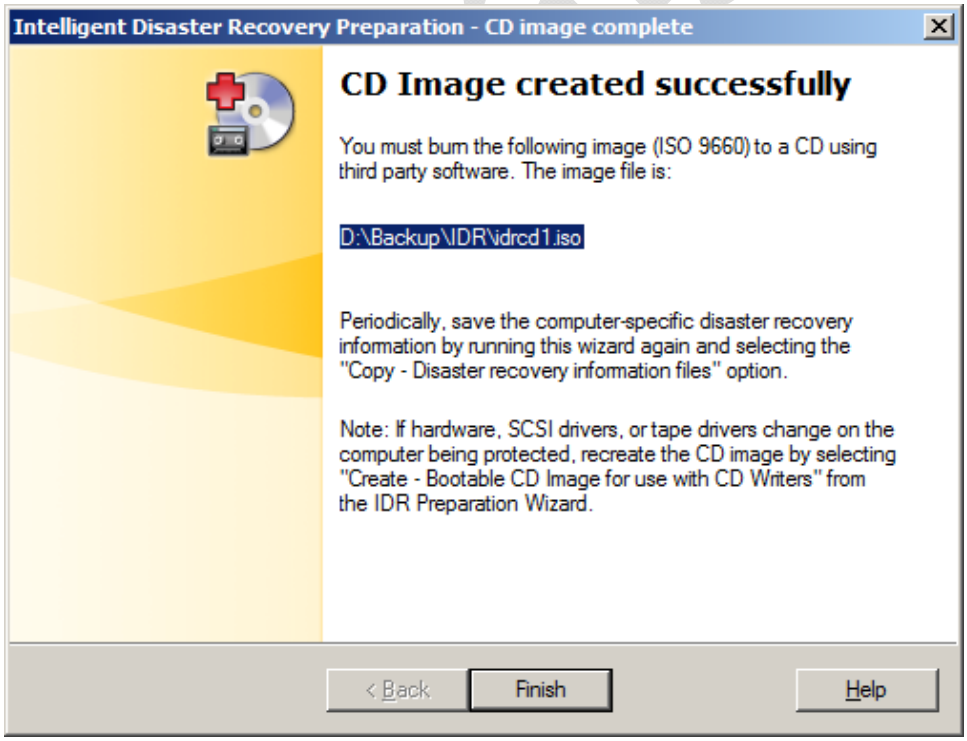


Figure 61. Screenshot. Identification of Image File Name and Location

.dr Files

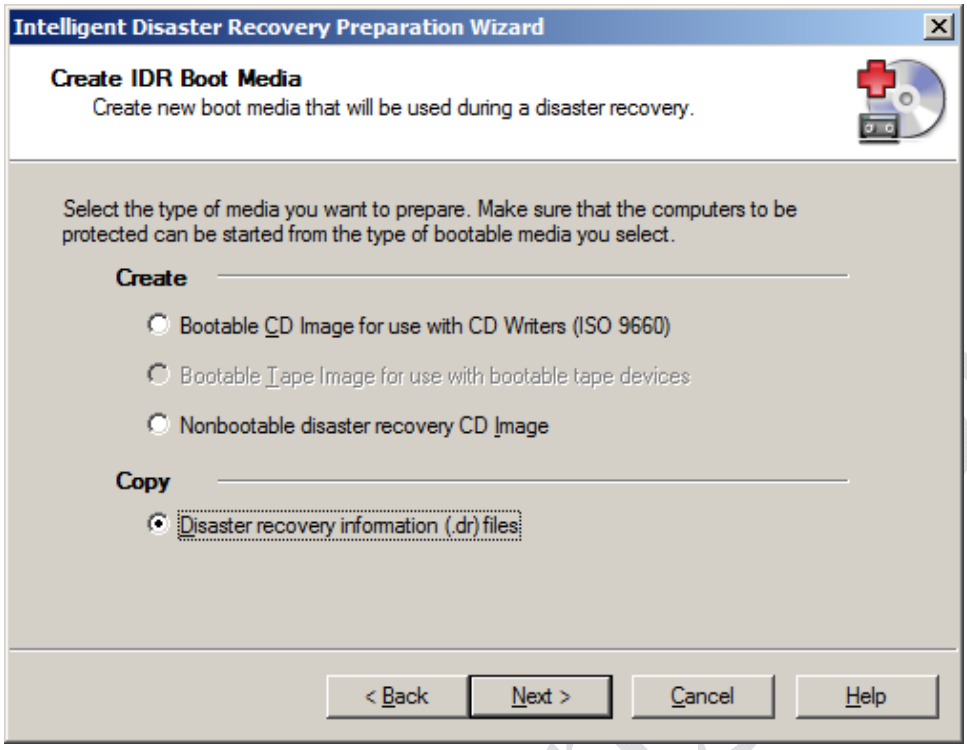


Figure 62. Screenshot. Selecting the Disaster Recovery File Option in the IDR Preparation Wizard

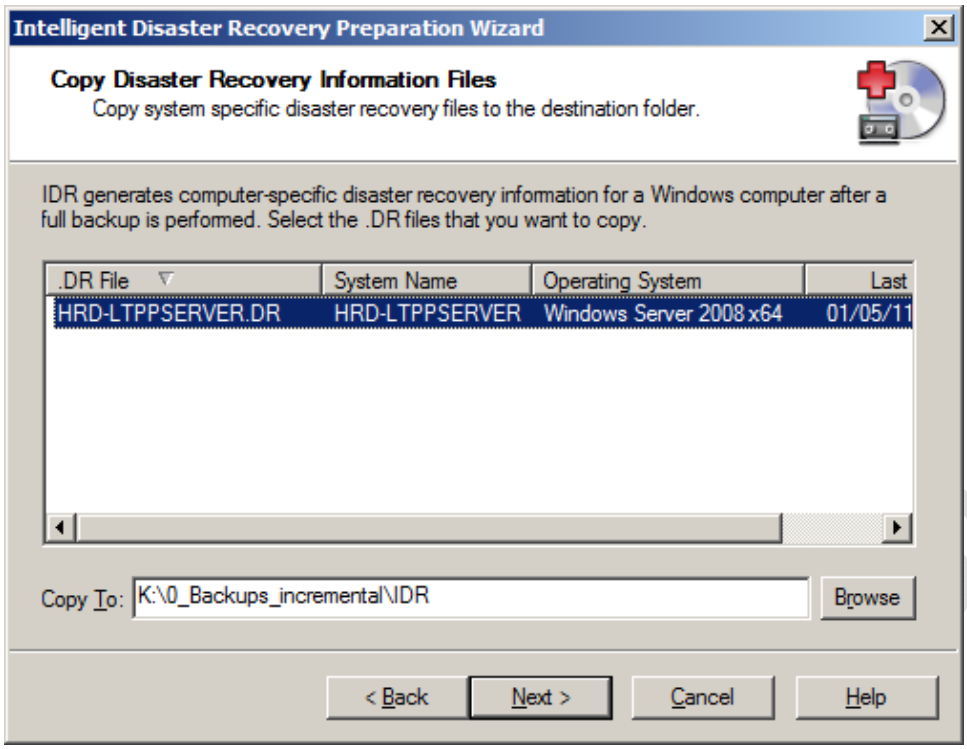


Figure 63. Screenshot. Identifying Computer and Location for .dr File

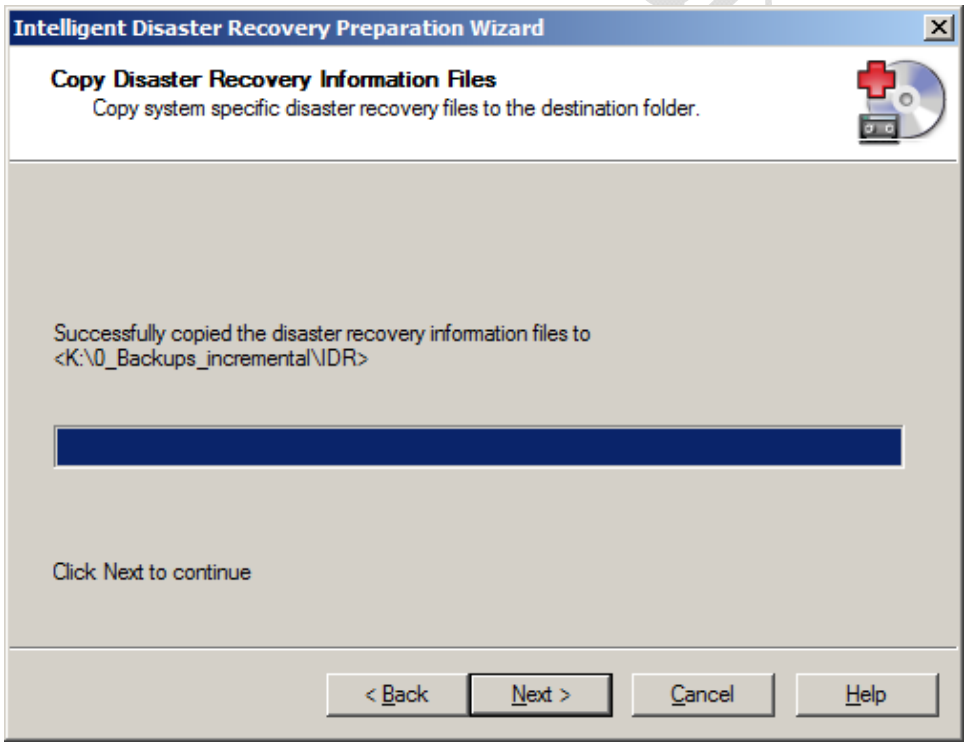


Figure 64. Screenshot. Completion of Creation of Copy of .dr File

Figure 65. Screenshot. Completion of Disaster Recovery Preparation

WORKING WITH MEDIA AND DEVICES

Symantec uses media and devices in a way that is specific to the software. Media refers to the files created in making a backup. Devices may be hardware or simply folder locations on a hard drive.

Media

Media are accessed through the Media tab. A media set is the collection of files (media) related to a specific backup activity. For the LTPP server, media sets have been defined to correspond to the various backups. There are other media sets (Imported, Retired, Scratch, On-line, Off-line) that are native to BE.

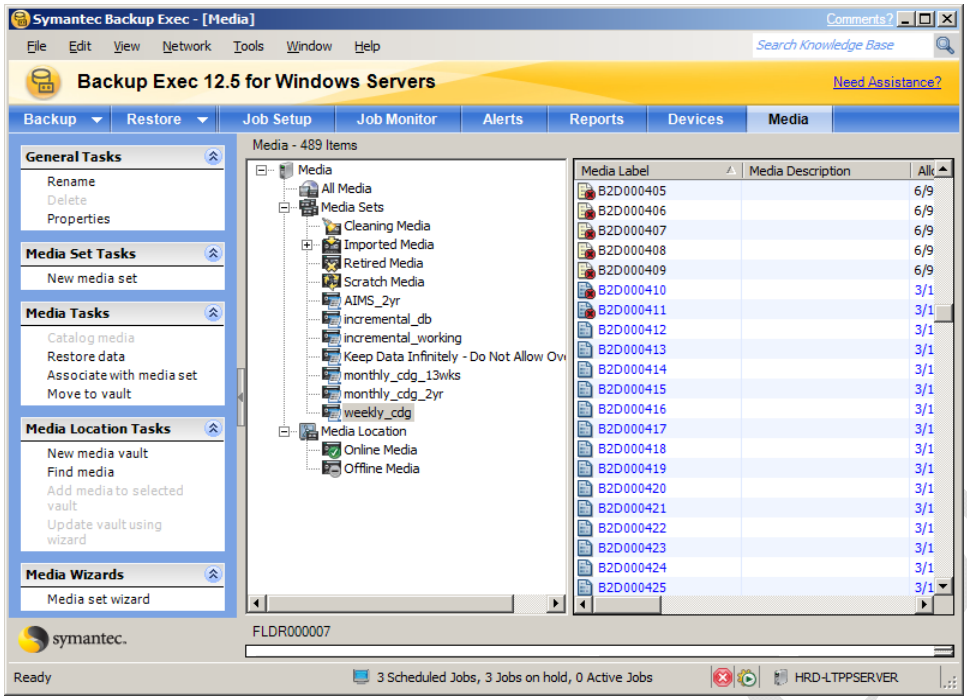


Figure 66. Screenshot. Main Media screen.

Each file that is part of a media set is listed in the right hand box when that media set is selected from the folder list in the center of the screen. Media have unique labels assigned by the software. The color coding associated with the label indicates whether the file can currently be overwritten (reused), appended or not overwritten. Blue indicates media available to be overwritten. A media icon with a circled red X in the lower right corner is off-line.

Media sets may be on-line or off-line. An on-line set is one that is physically on the computer on a hard drive or cartridge. An off-line set is one that is on a cartridge not in the cartridge drive.

Media may be moved between media sets. This may occur when a different folder structure is selected to store files on a hard drive or when media fail. A media failure is typically identified when a backup up fails. The most common error message is “Not appendable (End marker unreadable)”. In this case the media are moved to the “Retired” media set.

To move media select the media and right click on the name. A menu will come up as shown in the lower right portion of Figure 67.

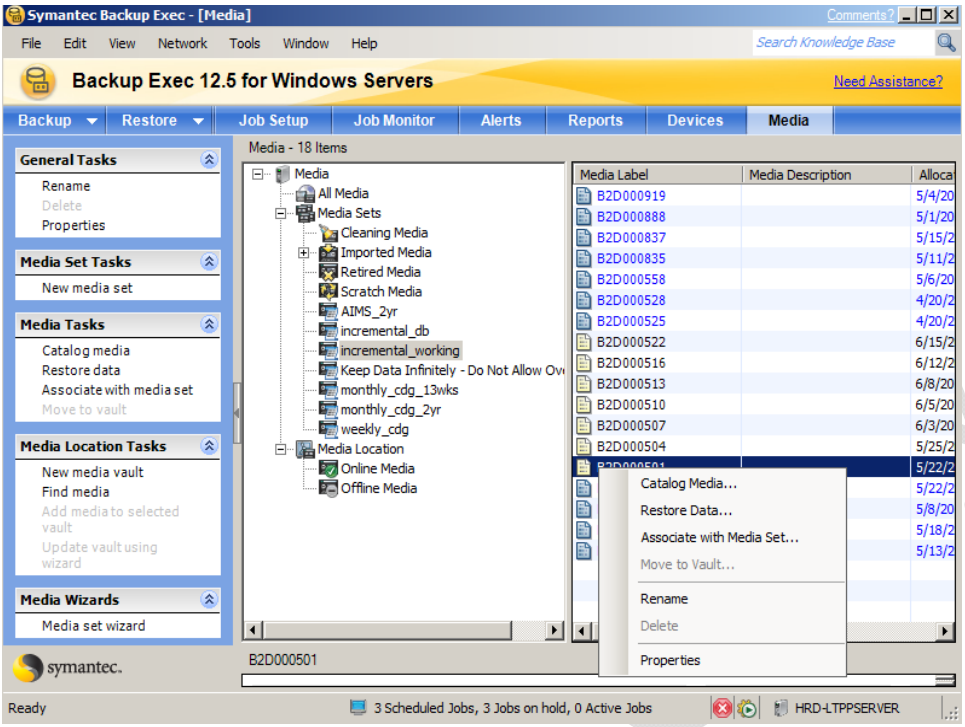


Figure 67. Screenshot. "Retiring" Media.

Click on “Associate with Media Set” in the dialog box shown in Figure 68.

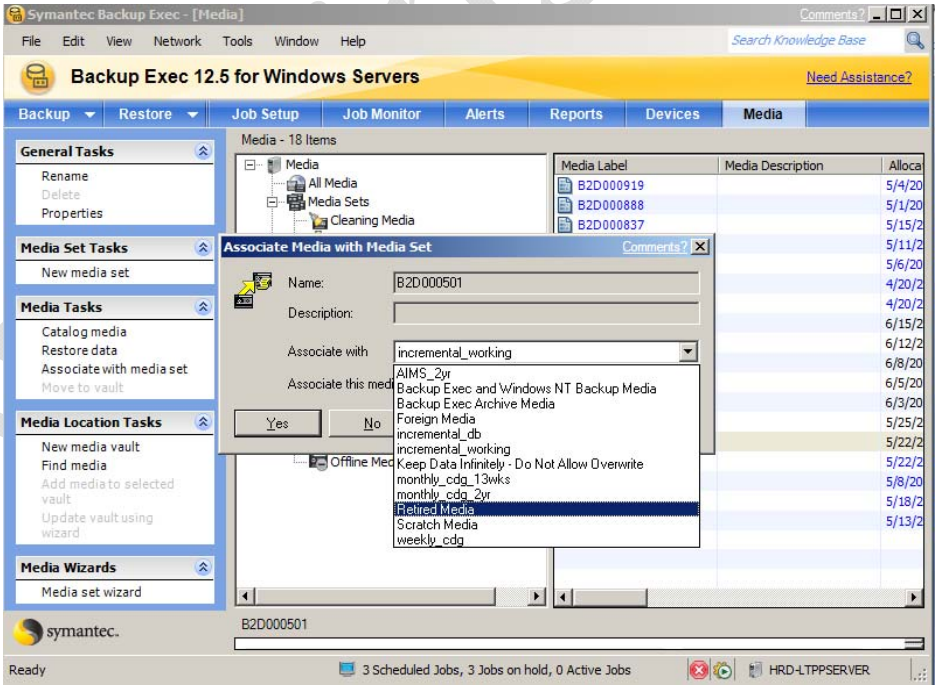


Figure 68. Screenshot. Select a new media set association.

Click on the arrow next to the block labeled “Associate with” when the next dialog box comes up. This will bring up a list similar to that shown in …...

Select and Click on “Retired Media”. It will then appear in the box next to “Associate with”.

Click on Yes on the dialog box (lower left corner) to confirm the selected media set.

The media will be removed from the current list and show up on the media list selected. In this case the list will be retired. The file has not been moved on the server/cartridge, it has just been made permanently unavailable for backup use.

A media set can be defined by using New media set under Media Set Tasks or Media set wizard under Media Wizards on the left side of the screen.

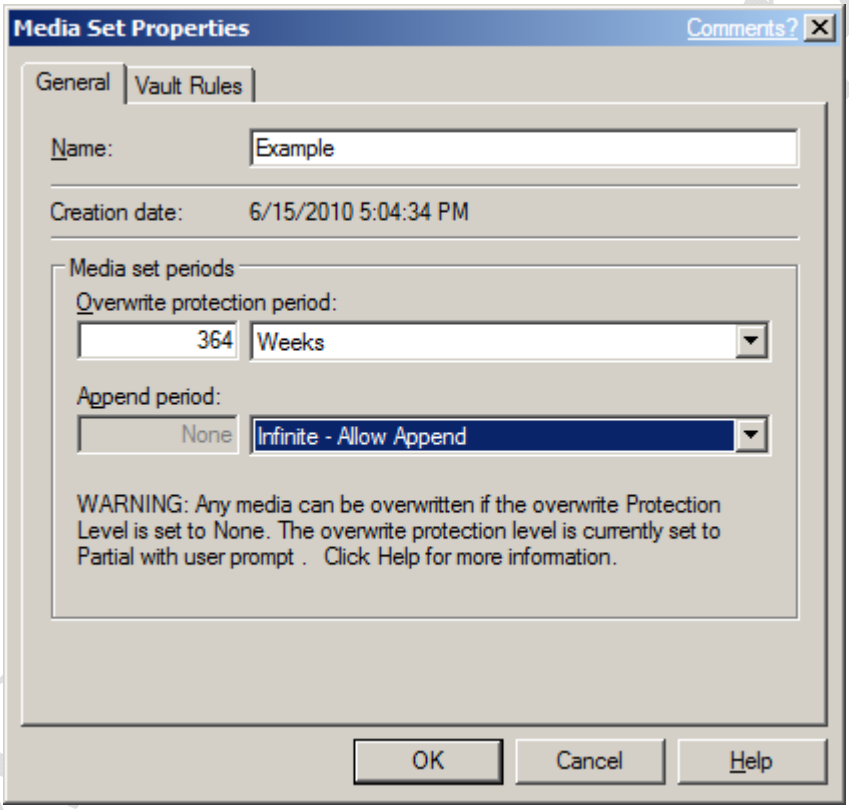


Figure 69. Screenshot. Setting media set properties.

In creating a media set three things are established, its name, the overwrite protection period and the append period. LTPP does not currently use the Vault options. The name reflects the content and frequency of the backup being included in the set. The overwrite period is set to 1 week less than the backup retention period. This value must be integer. This is set so that in the event a backup failure occurs and the backup is run later than anticipated, the media will be available when the next backup is expected. The append period is set to Infinite since either the cartridge will be removed before the next backup requiring a cartridge, or the amount of time to “fill” the media is unknown.

Devices

There are two devices for the LTPP server, a DELL RD1000 cartridge drive and the TB storage unit. The TB storage unit has a folder, 0_Incremental_backups in which all the "devices" exist. Each named folder is treated as a separate device. Multiple folders are strongly suggested so that if one of a set of nightly backups fails, it does not cause the other backups to be missed because the "device" is unavailable due to the failure. Devices can be found and their contents inventoried under the Devices tab in BE as shown in Figure 70.

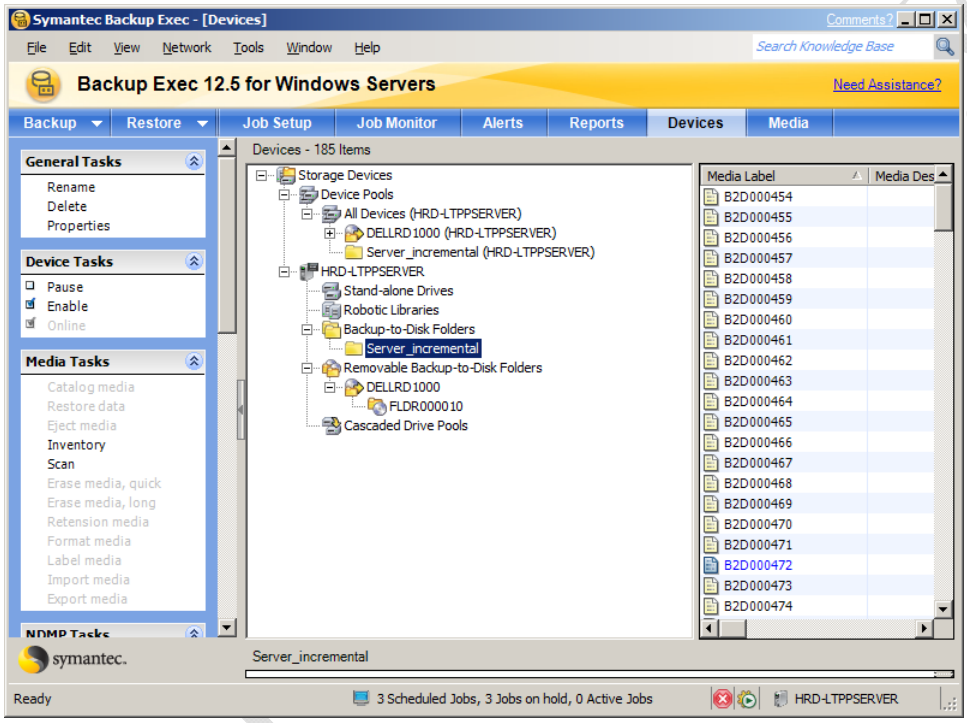


Figure 70. Screenshot. Device Options

Moving files (media) in Windows Explorer or other tools does NOT have any impact on where BE things the files are. If files are moved between Back-up-to-Disk Folders using Windows Explorer, each of the affected folders should be inventoried using the Inventory option after all the moves are completed. This also includes after deletion of "retired" media. (See the Media section for a discussion of "retired" media.)

It is recommended that cartridges be Ejected using BE rather than using Windows Explorer so that BE will track on-line and off-line data correctly.

APPENDIX H. OFF-SITE BACKUP PROCESS

FIRST FEDERAL CORPORATION (FFC)

All activities are done through the FFC web site. They consist of logging in, checking the inventory, creating batches and ordering additional boxes and labels as needed.

Logging in

Go to https://cmsnet03.ffederal.com

User ID: 700

Password: fha700

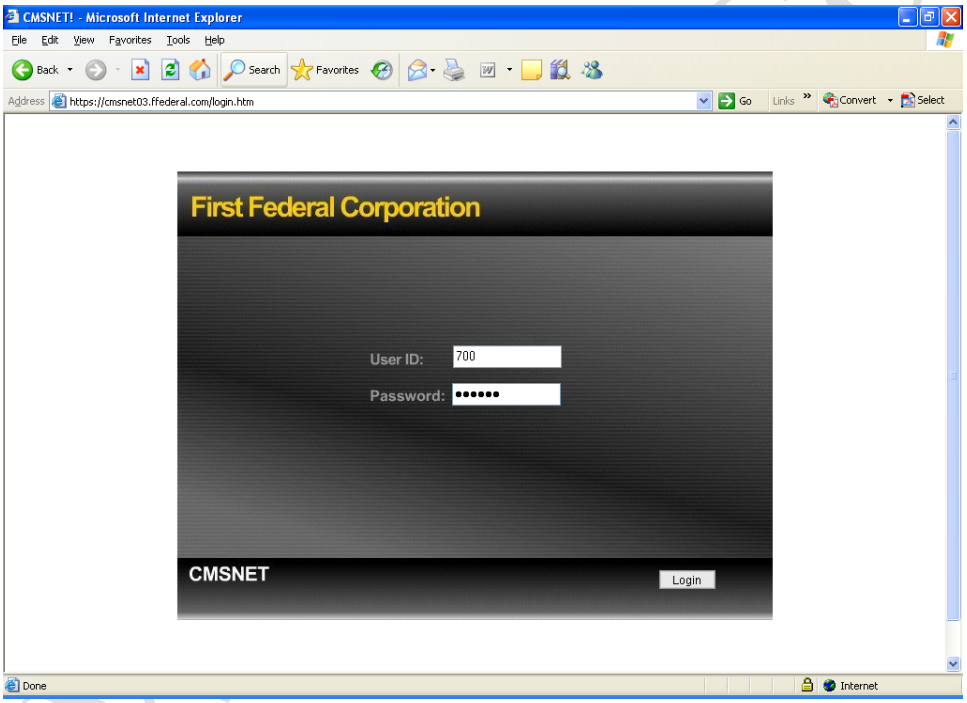


Figure 71. Screenshot. Login Screen for First Federal Corporation (Off-site Storage)

Type in the middle three characters of the code on the FFC security badge.

Figure 72. Screenshot. Secondary Login for First Federal

You may get an error message as shown below:

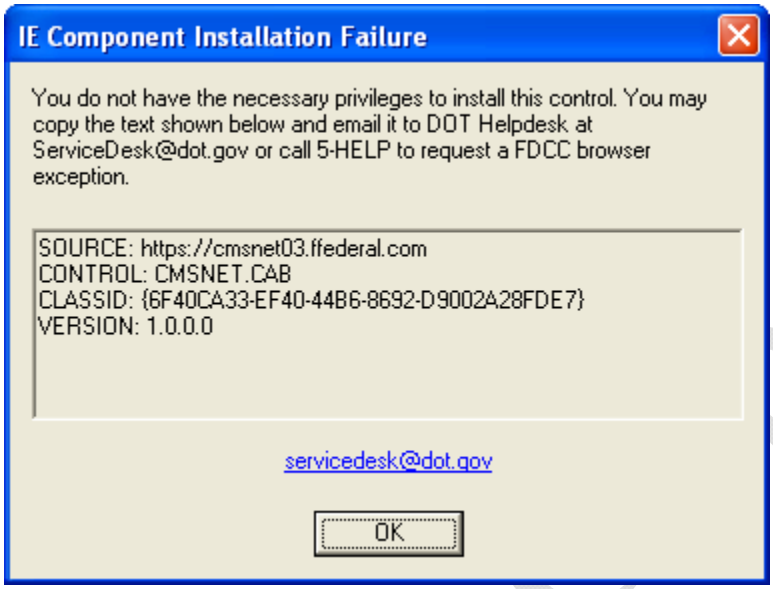


Figure 73. Screenshot. Error message on login to First Federal.

This error will have no impact on processing. It has been discussed with IT and they won't make any changes.

Checking Inventory

The boxes stored at First Federal and their content can be checked on-line.

Preparing a Batch

On the left panel of the screen and under Table of Contents, click on **Manual Entry**.

Then, on the right panel, click on "Start New Empty Batch". A batch is a set of media(boxes) that are all the same type in FFC terms. Note that the Vault number 700 is the default for the FHWA LTPP Account. The Type is Distribution to First Federal. The other type is Return from First Federal and only used for unscheduled returns. The Media option selected in this example is Container, Small.

There are a number of options, the default being 4mm. When selecting the media for an LTPP batch the option is determined by the fourth and fifth characters of the label. 700-CXNN-XXXXX as underlined. For CS use Container, Small. For CM use Container, Medium and for CL use Container, Large. Each media type requires a separate batch.

Under Volser type in the label of the container, 700-CXNN-XXXXX. Only boxes which are at FHWA or not in inventory when the batch is created can be added. If a box on hand is being sent and a box of the same size is being received and sent back the same day they

will be in different batches. The box on hand is in the batch created on the 3rd Monday. The box being received and sent back the same day will need a batch created on the day of delivery (Thursday morning.) Failure to do so will result in a discrepancy e-mail from FFC and a need to update the inventory to account for the unscheduled return.

Under A/R (Archive/Return) leave the selection Return. This indicates that the box will come back on the return date specified.

Under return date enter the 3rd Thursday of the month the box should come back to FHWA. This date can be found from the box rotation schedule which has been linked to the tape rotation schedule. A pop up calendar exists for date selection.

Add another box (volser- volume serial number) if needed. A separate batch must be created for each container size. The post upload pickup in August or September will generally need multiple batches to cover all the boxes.

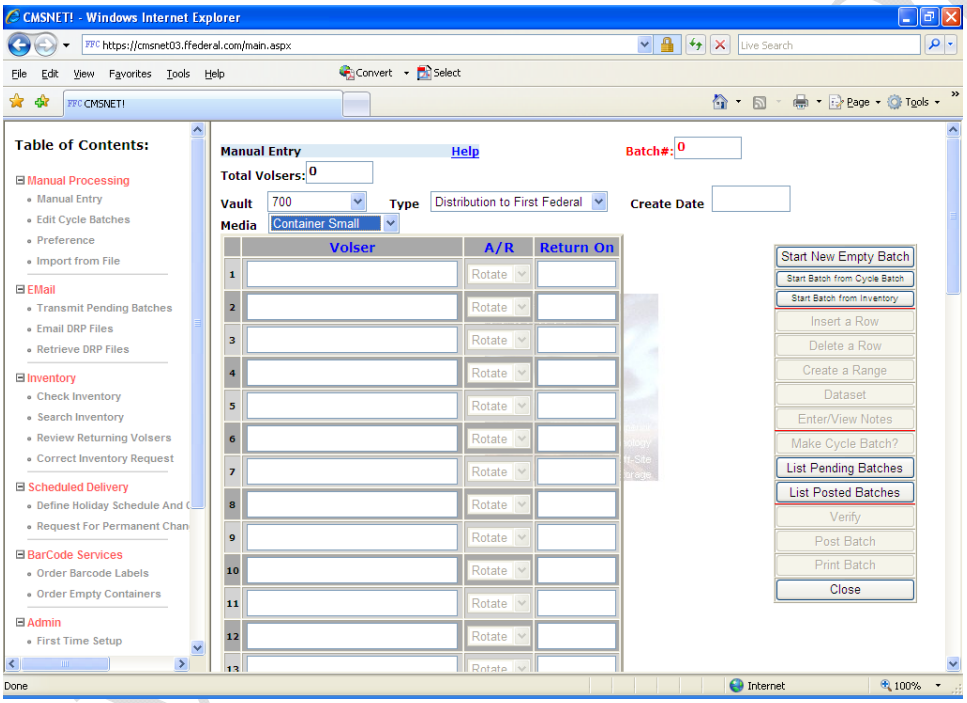


Figure 74. Screenshot. Preparing to add a batch for pickup by FFC.

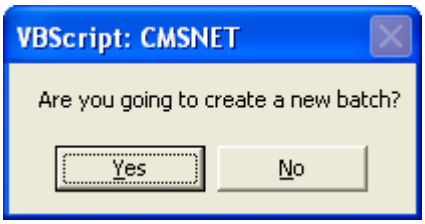


Figure 75. Screenshot. Confirmation to start add batch operation.

Click Yes.

After all data has been entered, click on **Dataset** on the right panel to enter a note which applies to the content of the box. This makes it possible to review the inventory without having any of the tape rotation materials on hand to flag a memory of their content.

Then, click on **Post Batch** on the right panel to post the first container. Repeat for additional container sizes.

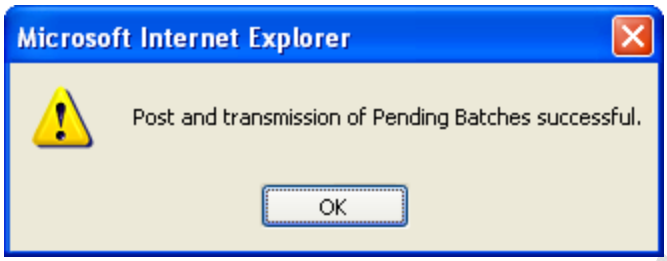


Figure 76. Screenshot. Confirmation of successful batch posting as pending.

Click OK.

After all batches have been posted, click Verify on the right panel to make sure Return On dates are future dates, etc.

Figure 77. Screenshot. Query to confirm batch verification.

Click Yes.

Click on Post Batch to send an email to FFC.

Figure 78. Screenshot. Confirmation query to post a batch as final.

The date in the message will be the pickup date. Click Yes.

The response is

Figure 79. Screenshot. Receipt Confirming Batch Posting

Click OK.

Getting boxes back

Ordering boxes and labels

OFF-SITE BOX ROTATION

While a general summary of content is included in the data stored on the site, a detailed listing of any given box's contents is printed for inclusion in the container.

Locks, combinations

APPENDIX I. SERVER RECOVERY – TFHRC SERVER

INTELLIGENT DISASTER RECOVERY

Intelligent Disaster Recovery is the method included in Symantec BE to support file restoration. It has two components, a bootable disk from which the computer can be restarted (or a new one brought up as a replacement) and a tracking system. The bootable disk should be created on at least a yearly basis or after a major system patch. The tracking file should be updated weekly prior to the weekly backup.

RESTORING A FILE

APPENDIX J. ORACLE DBA QUICK REFERENCE

This section includes instructions on a few functions that the DBA may encounter in normal operations. There is no way to document all possible situations. The on-line reference manuals for Oracle 12c are located through https://docs.oracle.com/en/database/database.html or at https://docs.oracle.com/database/121/nav/portal_5.htm. A screenshot with the Database Administration section highlighted is shown in figure 80. The "SQL Language Reference" and "Administrator's Guide" are two of the more frequently used manuals. Also included further down the list under Supporting Documentation is an Error Message document. PDF versions of the documents can be downloaded. Copies are kept on the server in the Software Downloads folder under Oracle.

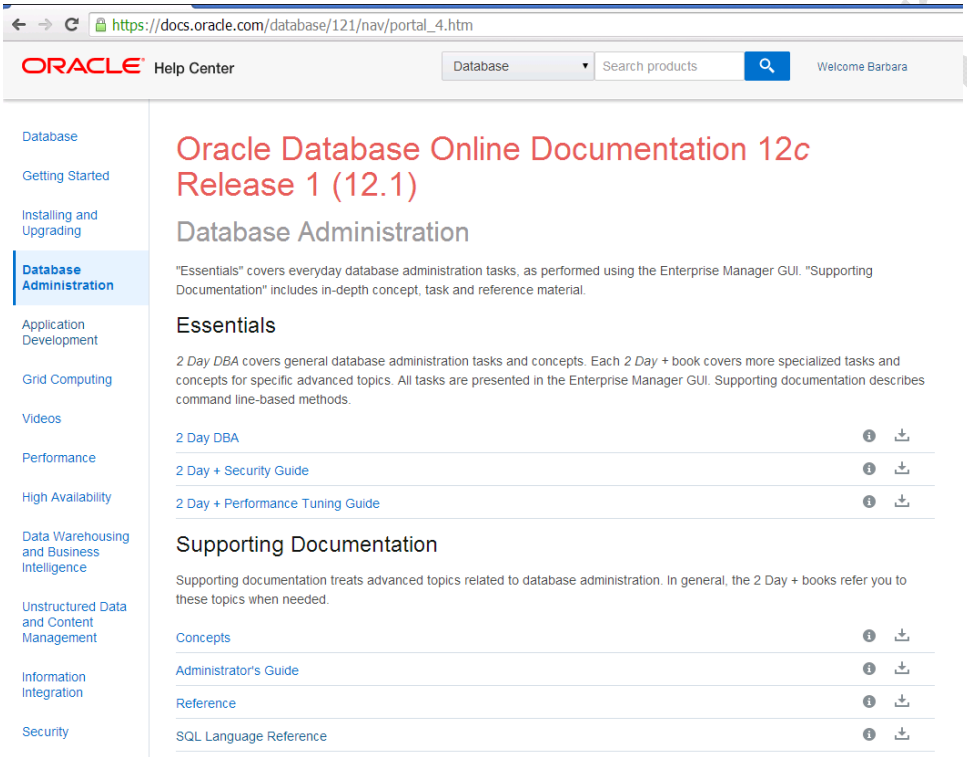


Figure 80. Screenshot. Online documentation for Oracle 12c – Database Administration.

Work on the database may be done at the command prompt in SQLPlus or using the DBA window in Oracle SQL Developer. In the sections which follow examples are limited to use of SQLPlus. The SQL Developer alternatives are discussed in the SQL Developer appendix. The included SQL scripts were taken from Oracle SQL Developer. The Oracle SQL Developer version used for this document was 4.0.3.16 for Java 1.7.0_55, Oracle IDE 4.0.3.16.84.

ORACLE ERROR MESSAGES

There are multiple ways to interpret Oracle error messages. A good starting point is using either the Oracle Error Messages document or to go directly to https://docs.oracle.com/database/121/ERRMG/toc.htm for Oracle 12c or http://docs.oracle.com/cd/E11882_01/server.112/e17766/toc.htm for Oralce 11g. This will give you a basic understanding of what the error is and its possible causes. Another technique in diagnosing errors is to look in the database's trace directory. The alert log and trace files located there may provide extra details about the error. Internet options include searches and My Oracle Support which requires registration and a license for Oracle support for most activities. A general web search may or may not provide additional information to resolve a problem.

DATABASE MAINTENANCE

Database maintenance is associated with sizing and running the database. DBA level maintenance can be done in SQL Developer using the DBA window. This panel is the DBA option under View on the toolbar for SQL Developer. Once a connection exists, a list of options will appear for the instance.

Install database

Record of database upgrade

Add tablespace

Listener issues including services starting.

Determine Characteristics of Tablespaces

Tablespace data dictionary views can be used to identify characteristics of tablespaces. A list of the views can be found in the Oracle Database Administrator's Guide[9]. More detailed information on each of them can be found in the Oracle Database Reference[10]. The most useful views are:

- V$tablespace – names
- DBA_Data_Files – files associated with each tablespace

Increase Tablespace Size

When a tablespace fills up, it will usually need to be increased in size to accommodate more data. Original tablespace sizes were estimated and a maximum size was dictated to avoid tablespaces growing very large without the administrator's knowledge. Determining which tablespaces have are approaching the maximum size may be done by

[9] Oracle 12c Oracle Database Administrator's Guide: http://docs.oracle.com/database/121/ADMIN/toc.htm

[10] Oracle 12c Oracle Database Reference on-line: http://docs.oracle.com/database/121/REFRN/toc.htm

running the Alter_db_size_auto.sql located in the synchronization directory. This script identifies all tablespaces that are at 90% of capacity and generates the scripts to extend the associated databases. Insufficient space may also be discovered on loading data during database synchronization. *(Discuss the script that identifies 90% full tablespaces. Add information on how failure may be found on loading data.)*

The syntax to increase tablespace size is -

```
ALTER DATABASE
DATAFILE 'path and database name.DBF'
AUTOEXTEND ON NEXT 256 MAXSIZE size in bytes/KB/MB;
```

Note that the name of the data file being extended is fully qualified and enclosed in single quotes. Typically, the LTPP databases extend data files rather than add them when expanding tablespace sizes. With SDR 29 some tablespaces have reached the maximum allowable database file size and must be extended by use of multiple files. As of SDR 29 the Undo tablespace could not be enlarged by expanding the initial database and additional files would need to be added to address storage issues.

Stop/Start the Database

There are two methods of starting and stopping the Oracle database instances. One method is to start and stop the corresponding Windows service. A second method is to use SQL*Plus.

The services are found through…..The names of these services all begin with "OracleService" and end with the instance name. Stopping the service will stop the instance and starting the service will start the instance. Starting and stopping can be done using the Windows control panel or using the "net start" and "net stop" commands in a command Window. When Windows starts, the services are automatically started and therefore the databases are running when the server starts. When a Windows shut down is required, during a power failure for example, the services will shut down which will cleanly shut down the databases.

The other method of starting and stopping the databases is to use SQL*Plus. This is a good method to use for performing cold backups, because it gives providesthe chance to perform some other housekeeping activities like creating backups of the parameters and control file. Shutting down the database only requires the "SHUTDOWN IMMEDIATE" command, but the commands below can make cloning and recovery easier.

```
SQLPLUS "/@IMSProd AS SYSDBA"
CREATE PFILE='BackupInitIMSProd.ora' FROM SPFILE;
ALTER DATABASE BACKUP CONTROLFILE TO TRACE;
SHUTDOWN IMMEDIATE;
EXIT;
```

Starting the database from SQL*Plus is equally easy. Just use "STARTUP".

```
SQLPLUS "/@IMSProd AS SYSDBA"
STARTUP;
```

```
EXIT;
```

Recover a Database

Database recovery can be a complex task. It tends to be needed when a cloning or database upgrade is done incorrectly.. Sometimes all it takes is the command "RECOVER DATABASE". When it works the "Database Recovered" message appears.

```
SQLPLUS "/@IMSProd AS SYSDBA"
RECOVER DATABASE;
EXIT;
```

Other times a slightly more complex version of the command is required. That is "RECOVER DATABASE UNTIL CANCEL". In this case each of the three redo logs are tried until the one that was in use when the database crashed is encountered.

```
SQLPLUS "/@IMSProd AS SYSDBA"
RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL;
G:\LTPP_Database\IMSProd\redo01.log
G:\LTPP_Database\IMSProd\redo02.log
G:\LTPP_Database\IMSProd\redo03.log
EXIT;
```

One of those two procedures will most likely recover the database. If they do not, an Oracle service request may need to be created to have them help in recovering the database or a recent backup may need to be restored.

TABLE MAINTENANCE

Due to the requirement to keep several databases in sync, it is not recommended that any tools other than SQL scripts be used to change the schema. SQL scripts provide a repeatable means of making changes to the schema. That does not mean that GUI tools such as Oracle Enterprise Manager (OEM) and SQL Developer are not useful. Both OEM and SQL Developer have tools to show the SQL statements necessary to recreate an object. For example, it is possible to make a change to an object using the GUI and click "Show SQL" instead of "Apply". A window will pop up showing the SQL that OEM would use to make the change. That SQL can be a good starting point in the generation of scripts.

Find tables and tablespace and owner – select owner, table_name, tablespace_name from dba_tables;

Find table ddl

Set long 5000; (need to have space to write out the answer)

Select sys.dbms_metadata.get_ddl ('Table', tablename, schema) from dual;

Add/Remove/Modify Field

See ALTER TABLE in the Oracle® Database SQL Reference 11g Release 2 manual for syntax options for this command. Some examples are as follows:

```
ALTER TABLE tablename ADD (newcolumn NUMBER(3,1));
ALTER TABLE tablename DROP COLUMN oldcolumn;
ALTER TABLE tablename MODIFY (smallnumber NUMBER(4,1));
```

The first statement would add a column called NEWCOLUMN as datatype NUMBER(3,1). The second statement would remove OLDCOLUMN from the table. The third statement could be used to change SMALLNUMBER from a NUMBER(3,1) to a NUMBER(4,1).

Modify Keys/Constraints

See ALTER TABLE in the Oracle® Database SQL Reference 11g Release 2 manual for syntax options for this command. Some examples are as follows:

```
ALTER TABLE tablename ADD CONSTRAINT pk_newtable
PRIMARY KEY (state_code, shrp_id)
USING INDEX TABLESPACE index_tablespace;

ALTER TABLE tablename DROP CONSTRAINT pk_newtable;

ALTER TABLE tablename disable CONSTRAINT fk_table_ref_cons;
```

The first statement would add a constraint to the table. This could be any type of constraint such as NOT NULL. The second statement drops the constraint that was just added. The third statement temporarily removes a constraint so that data can be added without considering parent child relationships.

Add/Remove Table

See CREATE TABLE and DROP TABLE in the Oracle® Database SQL Reference 11g Release 2 manual syntax options for this command. Examples of the basic statement are as follows:

```
CREATE TABLE newtable (
state_code  NUMBER(2,0) NOT NULL,
shrp_id     VARCHAR2(4) NOT NULL,
data        NUMBER(6,2)
CONSTRAINT pk_newtable
PRIMARY KEY (state_code, shrp_id)
USING INDEX TABLESPACE index_tablespace
)
TABLESPACE table_tablespace;

DROP TABLE newtable;
```

The first command creates a table, in the tablespace "table_tablespace," with STATE_CODE and SHRP_ID as the primary key with one column containing numeric data. The second statement removes the table that was just created.

Creating Public Synonyms

Public synonyms allow tables in other schemas to be referenced without specifying the schema. The full syntax of the Create Synonym and Drop Synonym commands is available in the Oracle® Database SQL Reference 10g Release 2 manual. LTPP instances generally work on the assumption that tables are referenced by public synonyms which are identical to the table name. Therefore, anytime a table is added or removed, the corresponding public synonym should be created or deleted.

The basic syntax to create a public synonym is as follows:

```
CREATE PUBLIC SYNONYM newtable FOR newtable;
```

This allows the table to be referenced by any user as if it were in their schema.

To remove a synonym, the following command is used.

```
DROP PUBLIC SYNONYM deletedtable;
```

USER ADMINISTRATION

User administration in Oracle involves privileges, passwords, and storage. It is important to understand the term user and schema are interchangeable. Privileges control whether or not the user can create tables or even connect to the database. Passwords should be unique for each user in an instance and between instances as well. Passwords for these users should be provided to the COR when an instance is established or the passwords are updated. Storage controls the amount of space a user can take in their default tablespace.

Oracle Users

The users in an instance can be identified with the following command –

```
Select username from all_users;
```

The core Oracle users are SYS and SYSTEM. Except for database creation, cloning or repair no work should be done with these user names. Other Oracle users may be created when an instance is created. LTPP practice is to lock all other accounts for security purposes. The accounts can be checked and locked using SQL Developer. To manually lock an account use –

```
Alter user username password expire account lock;
```

This command also sets the password to expired so that even if the account is subsequently unlocked, the user must know the old password and supply a new one to use the account.

LTPP Users

Standard LTPP users for instances on the TFHRC server are LTPPDBA, CustSupp, TRFDBA, Traffic, Consolidated, IPC, *Instance*User and DataCheck. LTPPDBA is the primary DBA and the schema under which the PPDB tables are created. TRFDBA is the DBA under which the LTAS schema was developed when LTAS and the PPDB were in separate instances. CustSupp is the schema originally associated with all customer support functions. Its use has been reduced to creation of a schema associated with database extractions for public dissemination. Traffic is a user associated with early versions of LTAS. It has been retained in lieu of recoding the software to ignore the tables in the Traffic schema. Consolidated is a schema used for materialized views that consolidate information from multiple tables. IPC is the schema used for objects that exist primarily of the use of the InfoPave™ application. *Instance*User is a user name prefaced with the instance short form name. This user can do most manipulations on most common objects within the database and is the preferred user for general work in an instance. Datacheck is a user that can look at but not alter objects in the instance.

Other users may be created on an as needed basis.

Identifying Users

The users for an instance can be identified using the All_Users view.

```
Select * from All_Users order by UserName;
```

Additional information about the roles and privileges granted users may be obtained using DBA_Role_Privs, DBA_SYS_Privs and DBA_Role_Role_Privs discussed later in this appendix. There is no way to determine what a user's password is. Lost passwords must be reset.

A script, user_review, is stored in the synchronization template for use in finding the users in any instance, particularly the cloned ones. It is run iteratively to both identify users and to set the passwords for the cloned instance.

Manage Users

Users are created using the CREATE USER command and given privileges with the GRANT command. A quick way to create a user who can create tables in the database's default tablespace and default temporary space is to use the GRANT command. For example,

```
CREATE USER newuser IDENTIFIED BY newpwd
DEFAULT TABLESPACE user_tablespace temporary tablespace temporary_ts;
```

This creates a user who can connect to the database as *newuser* with *newpwd* as the password. The specification of a user_tablespace puts all objects the user creates in a tablespace other than the SYSTEM tablespace. Typically the user_tablespace name for LTPP users is User_Data (11g) or Users (12c). The temporary tablespace name is Temporary_ts (11g) or Temp (12c)

After creating a user, privileges with at the system or object level can be granted. Privileges may be granted to individual users or to roles and the roles granted to users. LTPP practice is to grant privileges to roles and then grant roles to users. All users are granted the select_only role which allows connection to the database and the ability to query any table. The command is –

```
GRANT Select_only to newuser;
```

Other roles are discussed in a later section.

Removing users is accomplished with the DROP USER command. For example,

```
DROP USER newuser CASCADE;
```

will remove the user *newuser* from the database along with any tables owned by *newuser*. The word CASCADE can be left off if the tables will be deleted manually before dropping the user. This can prevent accidentally dropping tables owned by *newuser* and used by others.

Resetting a password can be accomplished with the ALTER USER command:

```
ALTER USER username IDENTIFIED BY newpass;
```

This changes *username*'s password to *newpass*.

How to find out the tablespace assigned - DBA_Users - Default_tablespace, temporary_tablespace

How to find roles and privileges assigned – user_tab_privs, user_sys_privs, user_role_privs

Select grantee, table_name from DBA_tab_privs where grantee = 'DATACHECK'

Select * from DBA_Sys_Privs where grantee = 'DATACHECK'

Select * from DBA_Role_Privs where grantee = 'CUSTSUPP'

How to find which users exist –

Roles

Roles are a way to group system and object privileges to control user access and security of a database. It is more efficient to use roles when assigning privileges to users instead of individual privileges. Privileges on objects can be assigned to roles. This makes it simpler to assign the ability to select data from a new table by assigning that privilege to a role rather than assigning that privilege to every user in the instance that needs access to that table.

Identifying Roles

The roles that exist in an instance can be listed by using –

```
Select * from dba_roles;
```

The system privileges associated with a role can be listed by using –

```
Select * from role_sys_privs;
```

The object privileges that are assigned to roles can be listed using –

```
Select * from role_tab_privs;
```

The roles that are assigned to other roles can be listed using –

```
Select * from role_role_privs;
```

The ability to assign roles to other roles allows for a hierarchy of privileges and permits assigning different groups of privileges to different users.

Three useful roles are DBA, Select_Only, and Power_User. The DBA role is defined by Oracle and provides the ability to manage the database. It is being deprecated. To replace DBA on the TFHRC server three roles have been created: Junior, Senior and LDBA. They include most but not all of the roles assigned to DBA. The Select_Only and Power_User roles are maintained as part of the DPW. They are included on the TFHRC server for compatibility in loading DPW files. The role definitions on the two systems are not the same. The roles and privileges discussion in this document is limited to the TFHRC server.

The Select_Only role provides access to the database (Create Session) and the privileges necessary to read PPDB tables (Select any Table). It does not provide the ability to change any of these tables.

The Power_User role provides the ability to change the PPDB data in addition to reading it. The Power_User_Role has the Select_Only Role. A user granted Power_User does not need to be granted Select_Only also. The privileges granted to the Power_User include Insert any Table, Update any Table and Delete any Table. This user may modify data in tables but not make major changes to the instance. This use of any table functionality is to simplify the user's access to non-standard tables in an LTPP instance.

The Junior role provides basic functionality in manipulating the database beyond the capabilities of the Power_User role. The privileges include Comment Any Table, Create Database Link, Create Materialized View, Create Procedure, Create Public Database Link, Create Public Synonym, Create Sequence, Create Session, Create Synonym, Create Table, Create Trigger, Create View, Drop Public Database Link, Drop Public Synonym, Execute Any Procedure, Export Full Database, Force Transaction, Global Query Rewrite, Import Full Database, On Commit Refresh, Query Rewrite, and Unlimited Tablespace. The privileges remain limited to manipulating data and making individual rather than global changes to the database.

The Senior role provides the ability to manipulate or manage any object in the database including the tablespaces. In addition to the Junior role the Senior role is granted the privileges of Alter Any Table, Alter Tablespace, Alter User, Create Any Cluster, Create Any Index, Create Any Materialized View, Create Any Procedure, Create Any Sequence, Create Any Synonym, Create Any Table, Create Any View, Create Role, Create Tablespace, Create User, Drop Any Index, Drop Any Materialized View, Drop Any Procedure, Drop Any Role, Drop Any Synonym, Drop Any Table, Drop Any View, Grant Any Role, Lock Any Table, Redefine Any Table, Select Any Dictionary, and Select Any Sequence.

The LDBA role contains most of the higher level privileges of the DBA role that may be needed to work with an LTPP instance. The LDBA is assigned the Senior roll and the privileges Administer Database Trigger, Alter Any Sequence, Alter Any Trigger, Alter Database, Alter Profile, Alter Rollback Segment, Alter Session, Alter System, Analyze Any, Analyze Any Dictionary, Audit Any, Audit System, Backup Any Table, Become User, Create Any Indextype, Create Any Job, Create Any Trigger, Create Cluster, Create Indextype, Create Job, Create Profile, Create Rollback Segment, Debug Any Procedure, Debug Connect Session, Drop Any Operator, Drop Any Sequence, Drop Any Trigger, Drop Profile, Drop Rollback Segment, Drop Tablespace, Drop User, Execute Any Program, Flashback Any Table, Flashback Archive Administer, Force Any Transaction, Grant Any Object Privilege, Grant Any Privilege, Manage Tablespace, Merge Any View, Restricted Session, Resumable, and Select Any Transaction.

Privileges assigned to roles can be changed over time so the previous listing should be taken as current at the time this document was last revised.

Managing Roles

The Create Role, Alter Role, And Drop Role commands are used to create and remove roles. Information about these commands is available in the Oracle® Database SQL Reference 10g Release 2 manual. This section will concentrate on maintenance of the existing PPDB roles. Whenever a table is added or removed from the PPDB, the corresponding privileges of the SELECT_ONLY and POWER_USER roles need to be updated.

When a table is added, the roles need to be updated to grant privileges to those users assigned these roles:

```
GRANT SELECT ON newtable TO SELECT_ONLY;
GRANT INSERT, UPDATE, DELETE ON newtable TO POWER_USER;
```

These statements grant privileges to the roles instead of individual users. Any user who has the role will automatically get the privilege. This is similar for revoking privileges.

When a table is deleted, the privileges should be revoked before it is deleted.

```
REVOKE SELECT ON deletedtable FROM SELECT_ONLY;
REVOKE INSERT, UPDATE, DELETE ON deletedtable FROM POWER_USER;
```

EARLIER ORACLE VERSIONS

LTPP has been using Oracle software since version 5 at the beginning of the program. LTPP servers managed by the TSSC have versions 10g, 11g and 12c installed. This section discusses the applications and references requiring use of 10g or 11g.

Several LTPP standalone applications that run against the database for producing the standard data release and other deliverables are compiled against Oracle 10g or 11g dlls. As of SDR 29, the 2015 release, most applications have been ported to 11g. The affected applications include rec_cnt.exe, ExtractStandardDataRelease.exe, FHWASubmittal.exe, and the QC programs.

The central server has a copy of the Oracle 11g client so that the QC programs can be run. The only QC program that needs to be run at TFHRC is the ESALCalcQC.exe. All other QC is run on the DPW. FHWASubmittal.exe has not been modified since it was updated for the Dell 2900 on which the latest Oracle version is 11g. ExtractStandardDataRelease.exe was modified for other reasons for SDR 29 and runs under Oracle 12c.

The Oracle 11g documentation can be viewed at http://docs.oracle.com/cd/E11882_01/nav/portal_4.htm. The layout is similar to that for Oracle 12c.

APPENDIX K. DATABASE SYNCHRONIZATION

The recurring task is database synchronization.

Frequency: Quarterly - (January, April, July, October)

Tasking: PM?PI/Co-PI

References: *Oracle import/export functionality*

Oracle datapump

Software: Oracle, Notepad++ (or other text editor), rec_ct.exe (LTPP utility), Microsoft Excel®

Scripts: alter_db_size_auto.sql

RefreshDataTruncate.sql

RefreshDataEnableConstraints.sql

User_review.sql

RecCtSync.cmd

Filing:

- Server - G:\1_Synchronization\yyyymm – working files
- Server – K:\Historical_Database\YYYY\Sync\MM_Month – record copy

Coordination: The PM/PI will review the schedule at the beginning of the task order to establish extraction and delivery dates.

At the beginning of the month a synchronization is due –

- Confirm delivery with DPW DBA.
- Verify the location of the current copy of the record count program and edit batch files that reference it appropriately.
- Verify/create current quarter's folders for the server.
    - Server - G:\1_Synchronization/yyyymm (working copy) with subfolders for each instance.
    - Server - K:\Historical_Database\YYYY\Sync\MM_Month (archive)

- Verify G:\ folders have all necessary scripts which include the core listed above and any scripts, parameter files or batch files used in the prior synchronization by instance.

On receipt of files –

- Copy off logs and other supporting export information to synchronization folders in G:\ and K:\

- Verify that all tables, views and materialized views are in the correct schema. See the section on Instance Review for details of the process to be completed.

- Do a record count of existing instance tables. To run the record count program on the existing data for the LTPPDBA and TRFDBA schemas:

    - Ensure no $* tables exist by running purge recyclebin; and committing it.

    - Open a command prompt window in the directory 1_Synchronization and type the following command:

```
RecCtSync dbaUN/dbapwd@db tdbaUN/tdbapwd@db  sync_date instance_abbr
```

    Where dbaUN is the LTPPDBA schema's DBA username, dbapwd is the password for that user, db is the database instance (e.g., IMSProd), tdbaUN is the TRFDBA schema's DBA username , tdbapwd is the password for that user, sync_date is the year and month for the current synchronization in the yyyy_mm format used in the directory structure and instance_abbr is the name of the folder for the specific instance being checked.

    This will create two files in the 1_Synchronization\yyyy_mm\instance directory: Instance_ByTableLTPPDBA.lis and Instance_ByTableTRFDBA.lis.

The files should be imported into an Excel spreadsheet for record count comparisons with previous synchronizations.

- Compare pre-load record count to post-load record count from last synchronization.

- Compare pre-load record count to the incoming export log to verify tables expected and identify any expected count decreases.

- Clone the current production instance to K:\Historical_Database\YYYY\Sync\MM_Month for temporary storage. The local test and development instances may be cloned as well.

After the initial instance is prepped (IMSTest by preference)

- Verify a good backup of the current production instance.

- Run RefreshDataTrucate.sql at the SQLPlus prompt to lock tables, and disable constraints, triggers, truncate clusters and truncate tables.
    - Start SqlPlus
    - Connect as the DBA to the relevant instance
    - Type @RefreshDataTruncate.sql to start the script.
- Load data. The 12c databases have been set up with a single DBA user that is not the LTPPDBA or the TRFDBA but IMPEXPDBA given the DBA privilege which has been deprecated. Importing the data requires the following command:

```
Imp impexpdba/imxpexppwd@instance file=filename.dmp fromuser=schema1
touser=schema1 ignore=y log=imp_filename_YYYYMMDD.log

Where schema1 will be successively LTPPDBA, TRFDBA, CUSTSUPP,
TRAFFIC,
```

1. Enable constraints.
2. Run record counts.
3. Clone record database using the instructions in the NIMS Ops Manual.
4. Return hard drive for use in next synchronization.

Work flow

1. Verify the working folder, G:\ 1_Synchronization\yyyymm, has copies of the tools to be used:

LoadData.cmd	TST_Sample_Basic_Info.sql
RefreshData.cmd	LTE SQL
RefreshDataTruncate.sql	DCV SQL
RefreshDataEnableConstraints.sql	Reprocess_code_asgn_date.sql
	Computed parameters .dmp

2. Create current quarter's folder on the server - K: \Historical_Database\YYYY\Sync\MM_Month
3. On receipt of hard drive copy off logs and other supporting export information to folder on G:\.

4. Do a record count of existing instance tables.

5. Compare pre-load record count to post-load record count from last synchronization. If the counts do not match either determine the difference or export the tables for later analysis, overwrite of imported tables or submittal for use on the DPW. The action will be determined by the table affected and the reason for the difference.

6. Compare pre-load record count to export log to verify tables expected and identify any expected count decreases.

7. Clone the current production instance to the local test and development instances.

8. Run LoadData batch file to update the database.

9. Run any materialized view scripts.

10. Update any administrative and computed parameters tables that were received out of date or empty.

11. Run RefreshData.cmd

12. Run record counts.

13. Clone record database to development and test instances.

14. Make copy of files from G:\ in current K:\folder

15. Erase prior year's synchronization files for the same quarter.

16. Return hard drive for use in next synchronization.

Process is standard import to dev, then test, then prod. Clones not done unless working files from each instance have been exported for import.

Alter table for sizing, Check counts, log of import for failures,

Check Mview status, refresh and run statistics as needed. PROD as clean cop

Confirm good backup of production database

Once each backup is complete, the system administrator (SA) should review the backup logs and verify that the backup completed successfully and that there were no errors that would cause problems restoring the database. Before continuing with the data upload, database staff should check with the SA to make sure a recent good backup of the database is available.

Clone the IMSProd Database to IMSTest

Cloning the production instance at this point in the process allows database staff to go back to a pre-upload copy of the data to compare and contrast once the new data has been loaded. See Section **Error! Reference source not found.** of the NIMS Ops Manual for details of the cloning process.

Verify Media and Organize Upload Data

When the public data extraction is received, it is important to verify the contents of each upload and that all media are readable. Once database staff has verified that all data files are readable, uploaded files should be copied into the standard synchronization structure.

Review Selected Upload Files

CN output files and record count output files can indicate data problems. These files should be reviewed by the regions, but can also be reviewed centrally, if time allows. Check for the following when reviewing CN output files:

Output for each table will include either a list of sections that had changes or a statement that No sections had changes

Output for each table will include total number of records, number of records with correct CN, number of records with wrong CN, number of records that had CN updated, number of records with wrong CN that did not have CN updated

The total number of records should equal either the number of records with correct CN or the number of records with correct CN plus the number of records with updated CN. Other combinations of counts need to be investigated. Contact regions with questions

When reviewing record count output:

- Look for tables that have many records at RS < E.
- Look for tables with 0 records.
- Contact regions with questions.
- Review the export logs:
    - Check each module for extraction of all requested tables (generally all)
    - Verify that there were no errors on exporting.

Update Upload Processing Files

Run the commented out portion that counts constraints to determine if any constraints have been added or removed. Document the value found from running the count in the script with the date run.

- Disable any new constraints/foreign keys that could cause trouble while loading data
- Disable database triggers that might fire when data loaded into database
- Comment out truncate statements for tables that are not being uploaded.
- Add truncate statement for any new tables being uploaded.
- Enable constraints and triggers disabled in the StartUploadProcess.sql file.

Process Upload

Once these procedures have been updated, they will be executed as follows:

- Run StartUploadProcess from the synchronization directory in a DOS window using the following command:

StartUploadProcess dbaUN/dbaPW@database upload_date

where upload_date is the official upload date in yyyymmdd format.

- Review the output file for errors:
    - Scroll through the entire output file and verify that all constraints were disabled successfully ("Table altered.")
    - Verify that all triggers were disabled ("Trigger altered.")
    - Verify that the cluster ("Cluster truncated.") and all tables were truncated successfully ("Table truncated.")
- Run LoadUpload.cmd in a DOS window using the following command:

LoadUpload dbaUN/dbaPW@database upload_date

where upload_date is the official upload date in yyyymmdd format.

- Review the import log file:
- Compare the import files to the related export files. Any discrepancies must be investigated.
- Run FinishUploadProcess in a DOS window using the following command:

FinishUploadProcess dbaUN/dbaPW@database upload_date

where upload_date is the official upload date in yyyymmdd format.

- Review the output file for errors:

Scroll through the entire output file and verify that all constraints were enabled successfully ("Table altered.")

Instance Review

Database synchronization and cloning is dependent on correct assignment of Oracle objects to schemas to reduce loss of work in progress or duplication of object names. There are basically three classes of users in the LTPP instances, operational users, data release users and working users. Operational users are the LTPPDBA and the TRFDBA. These are the two schemas under which all of the tables associated with basic LTPP data operations are created. The tables and materialized for these schemas are typically listed in the LTPPTD table or the SDR_Table_Inclusion_List. Data release users include CUSTSUPP and IPC. The tables associated with these schemas are not separately catalogued in LTPP created tables. Working users consist of all the other named users with table, view and materialized view creation privileges. These are the users whose tables vary over time and can be easily lost on cloning a database. Prior to updating any instance, changes in these schemas need to be identified and non-standard tables exported for import after cloning. The process to clean up schemas and preserve working tables has several steps: identification of users, identification of objects that do not belong to operations users in their schemas, creation and editing of parameter files by user to either transfer files to another schema or save them for later import, editing a batch file to run the exports, and doing the exports. Details of the process follow. The scripts that should exist for each instance include:

- schema_check_*eabbr*sql
- non-standard_parfiles_*instanceabbr*.bat (export batch file)
- *Instanceabbr* _exp_*schema_yyyymm.par*
- Post_clone_load_*instanceabbr*.bat (import batch file)

1. Run the script schema_check_*instancename*.sql. This identifies all users and objects that do not belong to operations users. It lists the files associated with data release users. It also counts objects belonging to other users.

2. Check the script's output file to see if users have been added or dropped based on the previous synchronization's script output.

    a. If users have been added, add counts for that user to the count section and re-run the script before proceeding.

    b. If users have been dropped, comment out the associated export and import lines in the export and import batch files.

3. Check the script's output file to verify that a parameter file exists for each working user.

    a. If a parameter file does not exist because there are too few files to warrant a parameter file, verify that an export line exists in the batch file to run the parameter files, non-standard_parfiles_*instancename*.bat.

    b. If the parameter file does not exist because the user has been added since the last synchronization, create a parameter file and add a line for it to the export batch file or add an export command line to the export batch file. Add the appropriate line to the import batch file.

4. Check the script's output to verify that no unexpected files are associated with the operations users.

    a. If unexpected files exist, create a parameter file(s) to transfer the files to the appropriate user.

        i. Add the parameter file(s) to the export batch file.

        ii. Add the exported file(s) to the import batch file.

    b. If expected files exist that are not part of the designated list, verify that they are listed in the appropriate parameter file for export.

5. Run the export batch file non-standard_parfiles_*instancename*.bat.

6. Review all log files from export.

    a. If any exports fail, re-run them at the command prompt and edit the batch file to have the working syntax.

    b. If any tables have 0 rows exported,

        i. Drop the empty tables. Drop the tables with a script and log of output to document the action.

        ii. Comment out the import line in the import batch file if it is table specific or all tables in an export .dmp file have been dropped.

    c. Edit import batch file to reflect existence of data and files to reload in the event of cloning an instance.

Electronic Files Management

APPENDIX L. CLONING THE DATABASE

This must be done under the Administrator password on the central server to have the necessary privileges.

BEFORE CLONING FOR THE FIRST TIME

If the destination instance is brand new, a service will need to be created for the instance.

Create a new PFILE for the instance by copying an existing copy. For example, copy initimsprod.ora to initimstest.ora

```
Copy c:\app\ora_12c\product\12.1.0\LTPP\database\initDBName.ora.
c:\app\ora_12c\product\12.1.0\LTPP\database\initNewDBName.ora
```

For the remainder of this discussion it will be assumed that the initDBName is IMSPROD and the initNewDBName is IMSTEST.

If the pfile does not exist, create it from the spfile.

Edit the new PFILE and change “IMSPROD” to “IMSTEST” everywhere using a text editor (Notepad or Notepad ++)

Create the directories for the new instance

```
md g:\LTPP_Database\DB_name

md g:\LTPP_Database\DB_name\CONTROLFILE
md G:\LTPP_Database\DB_name\DATAFILE
md G:\LTPP_Database\DB_name\ONLINELOG


md g:\LTPP_Database\copies\DB_name
md g:\LTPP_Database\copies\DB_name\CONTROLFILE
md g:\LTPP_Database\copies\DB_name\ONLINELOG

md F:\LTPP_Database\copies\DB_name
md F:\LTPP_Database\copies\DB_name\CONTROLFILE
md F:\LTPP_Database\copies\DB_name\ONLINELOG

Where G:\ is the primary database location and F: is the backup file
location
```

Create the service for IMSTest

```
      oradim –new –sid IMSTest –syspwd sys4imstest –maxusers 50 –
startmode auto –pfile
“C:\app\ora_12c\product\12.1.0\LTPP\database\initNewDBName.ora”
```

The value of syspwd should be recorded for reference. Loss of the SYS password may require deleting and recreating the instance.

Enter the Oracle service user password when requested.

Edit C:\ app\ora_12c\product\12.1.0\LTPP\network\admin\tnsnames.ora. Duplicate the IMSProd entries (IMSProd and Listener_IMSProd). Change IMSProd to IMSTest in the copy.

Edit C:\ app\ora_12c\product\12.1.0\LTPP\network\admin\Listener.ora. Duplicate the IMSProd entry and change IMSProd to IMSTest in the copy

Restart the listener

```
lsnrctl stop
lsnrctl start
```

CLONING

Cloning is the duplication of a database. Throughout this discussion IMSProd is the source instance being cloned. IMSNew is the instance that is getting and exact duplicate (clone) of IMSProd.

Shut down the source instance to be cloned using the following syntax where each line is a separate entry. The initial line is executed at the command prompt. SQLPlus is called in the first line. The remaining lines are executed at the SQLPlus prompt.

```
sqlplus "sys/syspwd@imsprod as sysdba"
create pfile from spfile;
alter database backup controlfile to trace;
shutdown immediate;
exit;
```

Shut down the destination instance (if not newly created) using the syntax in the next three lines. The first line calls SQLPlus and the remaining lines run at the SQLPlus prompt.

```
sqlplus "sys/syspwd@imsnew as sysdba"
shutdown immediate;
exit;
```

Delete the files from the destination directories. Log on as Administrator to do this without having to check folder permissions. The syntax provided is run at the command prompt rather than using Windows Explorer to do the same thing.

(Check for location of trace files)

```
del G:\LTPP_Database\IMSNew\ONLINELOG
del G:\LTPP_Database\copies\IMSNew\ONLINELOG
del F:\LTPP_Database\IMSNew\ONLINELOG
```

Copy the source instance to the destination

```
copy D:\LTPP_Database\IMSProd\*.* D:\LTPP_Database\IMSTest
copy D:\LTPP_Database\IMSProd\Tablespaces\*.*
     D:\LTPP_Database\IMSTest\Tablespaces
```

Copy the online logs from the originating database locations to the new database. The original locations will typically be:

```
Copy G:\LTPP_Database\IMSProd\ONLINELOG\*.*
G:\LTPP_Database\IMSTest\ONLINELOG
Copy G:\LTPP_Database\copies\IMSProd\ONLINELOG\*.*
G:\LTPP_Database\copies\IMSTest\ONLINELOG
Copy F:\LTPP_Database\IMSProd\ONLINELOG\*.*
F:\LTPP_Database\IMSProd\ONLINELOG
```

Copy the original control files from the originating database locations to the new database.

```
Copy G:\LTPP_Database\IMSProd\CONTROLFILE\*.*
G:\LTPP_Database\IMSTEst\CONTROLFILE\*.*
Copy G:\LTPP_Database\copies\IMSProd\CONTROLFILE\*.*
G:\LTPP_Database\copies\IMSTest\CONTROLFILE
Copy F:\LTPP_Database\IMSProd\CONTROLFILE\*.*
F:\LTPP_Database\IMSTest\CONTROLFILE
```

Copy the data files from the originating database location to the new database.

```
Copy G:\LTPP_Database\IMSProd\DATAFILE\*.*
F:\LTPP_Database\IMSTest\DATAFILE
```

Create a SQL script to generate a new control file that identifies the clone database name and points to the new file location. Note that once this script is created, these steps only need to be repeated when new data files are added to the database. It is, however, good practice to create a new script every time a database is cloned.

A script to generate a control file is created with the following steps.

Find the trace file with the same timestamp as the “alter database backup controlfile to trace” command. This will be located in the source database’s trace directory. An example would be
“G:\LTPP_database\diag\rdbms\IMSPROD\IMSProd\trace\imsprod_ora_4124.trc”.

1. Save the file as
   “G:\LTPP_Database\IMSTest\Modifications\CreateIMSNewControlFile.sql”

2. Edit the trace file with a text editor, i.e. Notepad++ or Notepad.

a. Find the “Set #2. RESETLOGS case” section

b. Delete everything above the “STARTUP NOMOUNT” line

c. Find the “ALTER TABLESPACE” line and delete everything below it

d. Find the line with the ; (semi-colon) after CHARACTER SET WE8MSWWIN1252.

   i. Remove all lines down to ALTER DATABASE OPEN RESETLOGS

   ii. Remove all commented lines (lines beginning --_.

   iii. Remove the line - RECOVER DATABASE USING BACKUP CONTROLFILE

e. Change all occurrences of “IMSPROD” to “IMSNew” (the new instance name.)

f. Change path if necessary.

g. Change the “CREATE CONTROLFILE REUSE DATABASE” line to “CREATE CONTROLFILE REUSE SET DATABASE”

3. Save the file.

Execute the script to create the control file Execute the script to create the control file from the SQLPlus prompt and start the database. For the script to work the ora_12c user must have read write permissions on the included directories. Permission should be given at the LTPP_Database level.

The new instance is started by

- Executing the script to create the control file from the SQLPlus prompt.
- Changing user passwords
- Deleting LTPP created users not used in the instance.
- Adding the instance specific users. This is best done with scripts if object level privileges are granted.
- Creating a SPFILE and restart the database instance using it.

The sequence of commands from the command prompt is typically –

```
sqlplus “sys/syspwd@imsnew as sysdba”
```

Followed by a series of command executed at the SQLPlus prompt.

```
(if connected to an idle instance - Shutdown abort;)
@G:\LTPP_Database\IMSNew\Modifications\CreateIMSNewControlFile.sql
Alter user ltppdba identified by newpwd replace oldpwd (cloned db);
Alter user trfdba identified by newpwd replace oldpwd;
Alter user custsupp identified by newpwd replace oldpwd (cloned db);
Alter user system identified by newpwd replace oldpwd (cloned db);
Alter user datacheck identified by newpwd replace oldpwd;
Drop OriginatingInstanceUser on delete cascade;
Create NewInstanceUser identified by userpwd
      Default tablespace user_data
      Temporary tablespace temp;
Grant power_user to NewInstanceUser identified by userpwd;
Grant select_only to datacheck identified by datacheckpwd;
shutdown immediate;
create spfile from pfile;
startup;
```

Connect to the database from which the clone was made and start it.

```
Connect sys/syspwd@imsprod as sysdba
Startup open;
Exit;
```

If the listener does not know of the service when the attempt is made to log on do the following at the command prompt:

```
Lsnrctl stop
Lsnrctl start
```

APPENDIX M. SQL DEVELOPER NOTES

IMPORTING DATA

EXPORTING DATA

DATABASE MANAGEMENT

Tablespace Modifications

With a connection to the appropriate database in the DBA window, select the Storage option and then Tablespaces as shown in **Error! Reference source not found.**. Under Tablespaces a list of all tablespaces will appear. Selecting a tablespace will bring up details on it, a list of data files, free space information, a list of objects in it, a pie chart for usage and the SQL to recreate the tablespace. A example with a partial list of objects is shown in **Error! Reference source not found.**. Changing the tablespace size is done by selecting the Edit option on the Actions dropdown shown in **Error! Reference source not found.**. The dialog box that appears to edit the table space (**Error! Reference source not found.**) includes the name of the data file that will be expanded and the option to set the maximum size (Max Size) in kilobytes, megabytes, gigabytes or terabytes. Selecting the DDL tab in the Edit Tablespace dialog with the Update option chosen will display the SQL statement to make the changes made in the File Specifications window. A sample statement would be –

```
ALTER DATABASE
DATAFILE
'D:\LTPP_DATABASE\IMSDEV\TABLESPACES\MON_MEDIUM_TABLE_TS01.DBF'
AUTOEXTEND ON NEXT 256 MAXSIZE 90177536;
```

Where the new maximum size is shown in bytes (90177536). This can be edited to the appropriate multiple rather than computing the value in bytes if done manually. Note that the name of the data file being extended is fully qualified and enclosed in single quotes. Typically, the LTPP databases extend data files rather than add them when expanding tablespace sizes.

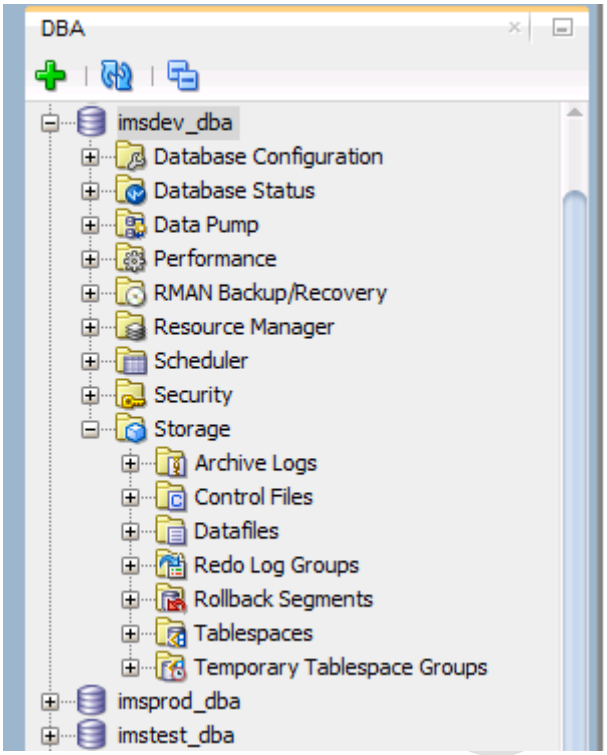


Figure 81. Screenshot. SQL Developer tablespace management.

Start Page | imsdev_dba | MON_MEDIUM_TABLE_TS

Details | Datafiles | Free Space | Objects | Usage Chart | SQL

Actions...

	OWNER	OBJECTNAME	OBJECTTYPE	SIZE	INITIALEXT	NEXTEXT	NUMEXTENTS	MAXEXTENTS
1	LTPPDBA	MON_DEFL_MASTER	TABLE	2016 Kb	1024Kb	96 Kb	21	2147483645
2	LTPPDBA	MON_DEFL_TEMP_VALUES	TABLE	5472 Kb	104Kb	96 Kb	57	2147483645
3	LTPPDBA	MON_DIS_AC_REV	TABLE	2304 Kb	2200Kb	96 Kb	24	2147483645
4	LTPPDBA	MON_DIS_CRCP_REV	TABLE	1248 Kb	1216Kb	96 Kb	13	2147483645
5	LTPPDBA	MON_DIS_JPCC_FAULT	TABLE	8256 Kb	4544Kb	96 Kb	86	2147483645
6	LTPPDBA	MON_DIS_JPCC_FAULT_SECT	TABLE	3456 Kb	3456Kb	96 Kb	36	2147483645
7	LTPPDBA	MON_DIS_JPCC_REV	TABLE	1536 Kb	1464Kb	96 Kb	16	2147483645
8	LTPPDBA	MON_DIS_PADIAS42_AC	TABLE	1728 Kb	1656Kb	96 Kb	18	2147483645
9	LTPPDBA	MON_DIS_PADIAS42_CRCP	TABLE	1248 Kb	1216Kb	96 Kb	13	2147483645

Figure 82. Screenshot. Object list under Tablespace in SQL Developer DBA window.

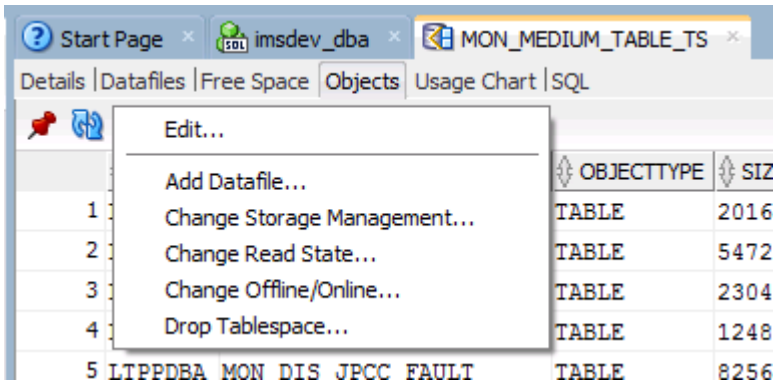


Figure 83. Screenshot. Actions... dropdown.

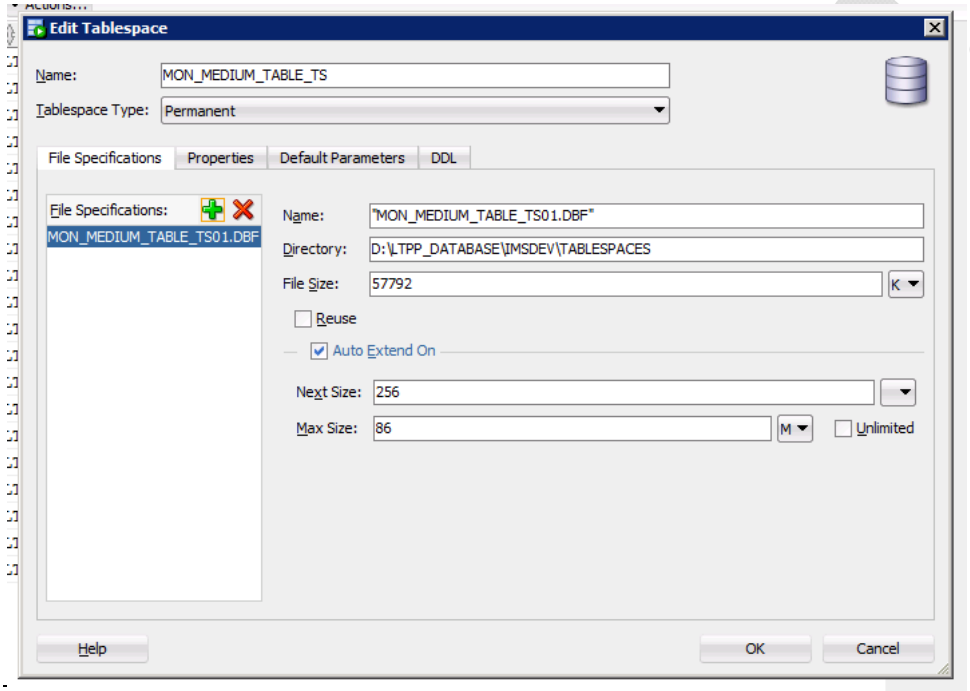


Figure 84. Screenshot. Edit Tablespace dialog box - SQL Developer.

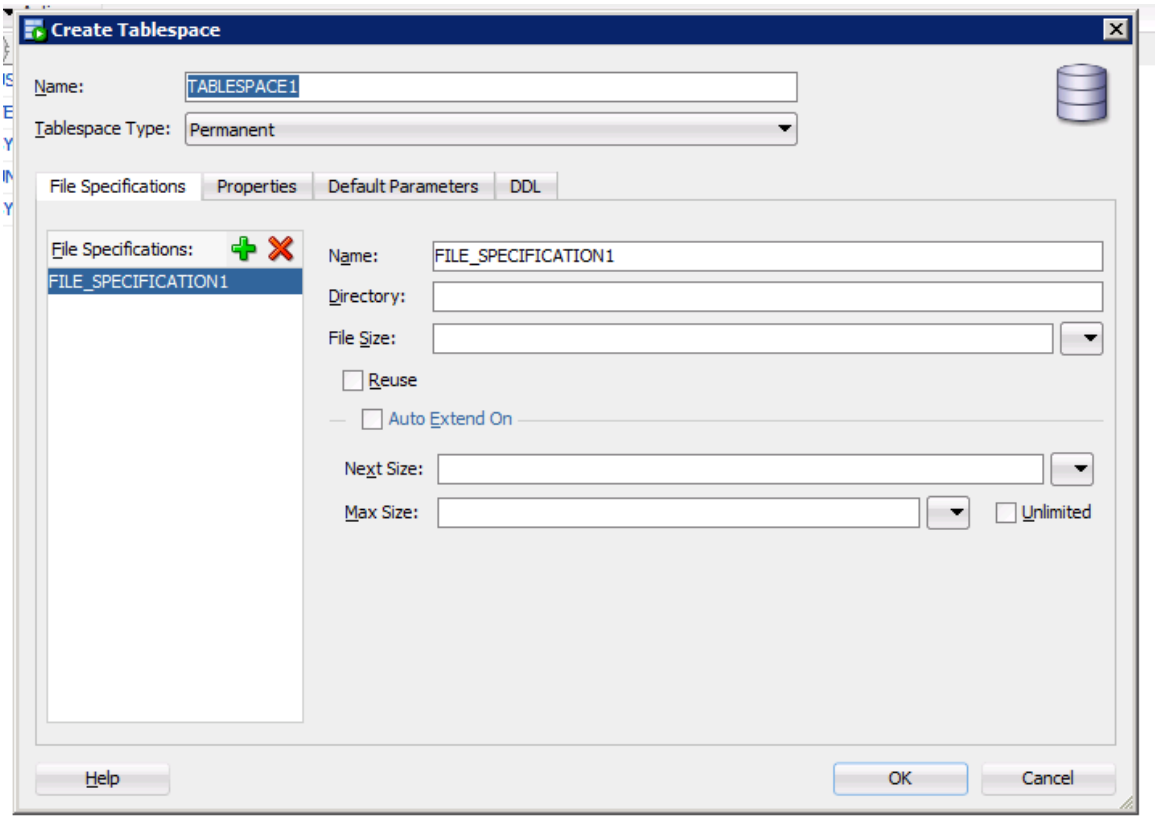


Figure 85. Creating a new tablespace.

USING SCRIPTS

SETTING UP CONNECTIONS

MANAGING USERS

Users can be created, dropped and modified within this utility by users with sufficient privileges. Once a user is connected to an instance the other users can be identified by clicking on the Other Users folder at the bottom of the users folder list. Right clicking on the Other Users label brings up options to refresh, filter, clear filter, create user or drop user.

In creating a user the user name and password is assigned at a minimum. In addition the user should be assigned User_Data as a default table space and Temporary_TS as the temporary .

Locking a user with SQL Developer is done after connecting using a DBA account. If the connection is made through the Connections window, the users may be found under Other Users, the last option on the list under the DBA objects. If the connection is made through the DBA window, Users can be found under the Security options as shown in figure 86.

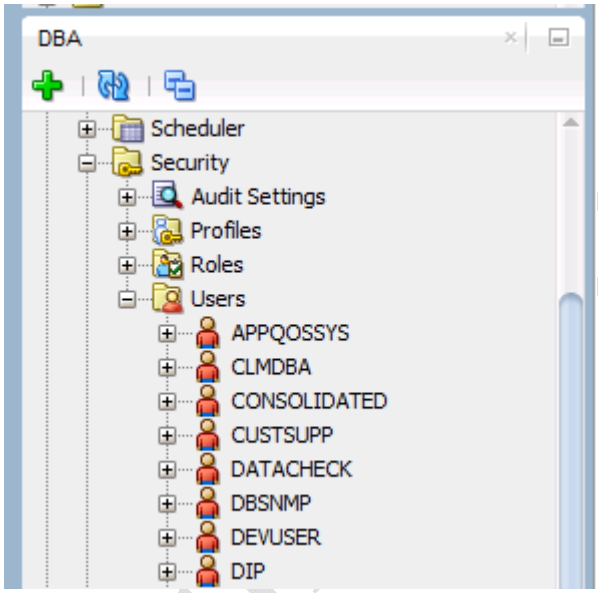


Figure 86. Screenshot. SQL Developer DBA location for users to manager user properties.

Left clicking on a user name brings up a screen like figure 87 where account status can be checked. In the example the account status is Open. Right clicking on a user name or the Actions… drop down brings up the list in figure 88 that allows editing properties for a user. Selecting Lock User is the simplest way to lock an account. Clicking on Apply on the next screen to appear will make the change.

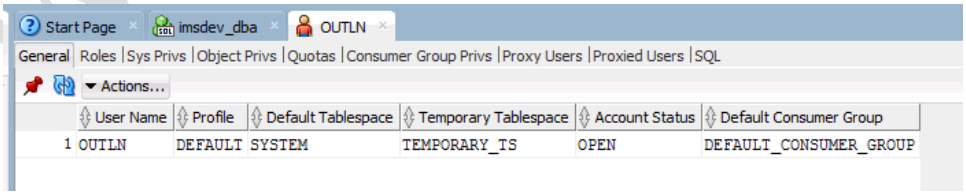


Figure 87. Screenshot. General user information in SQL Developer.

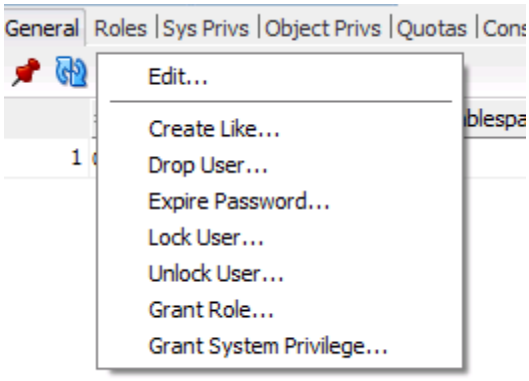
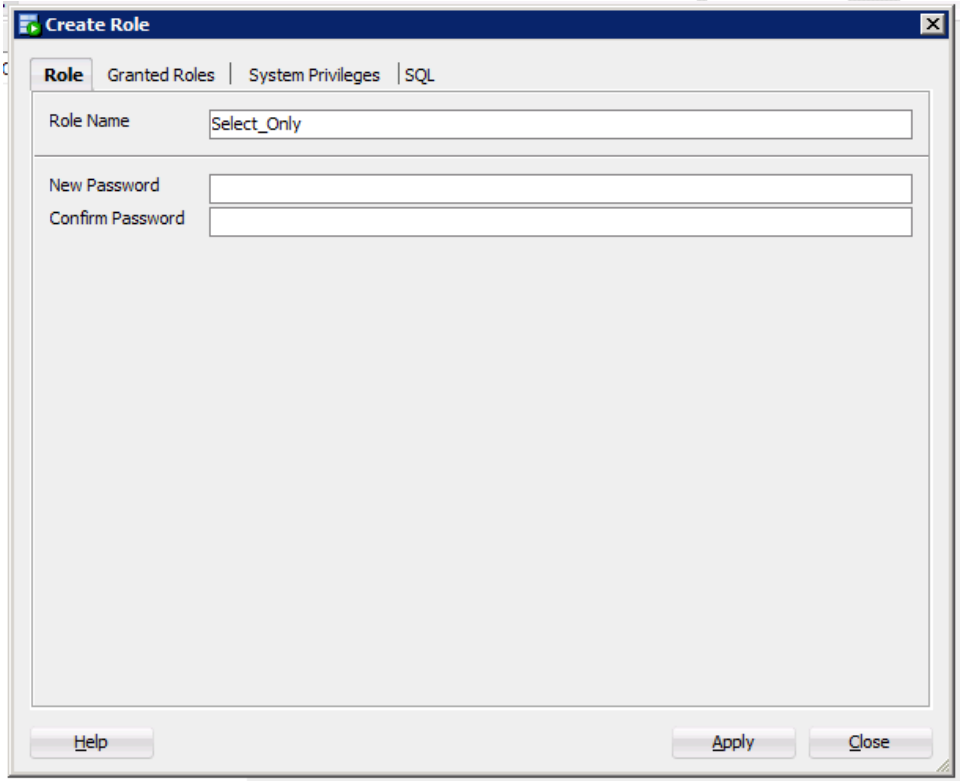
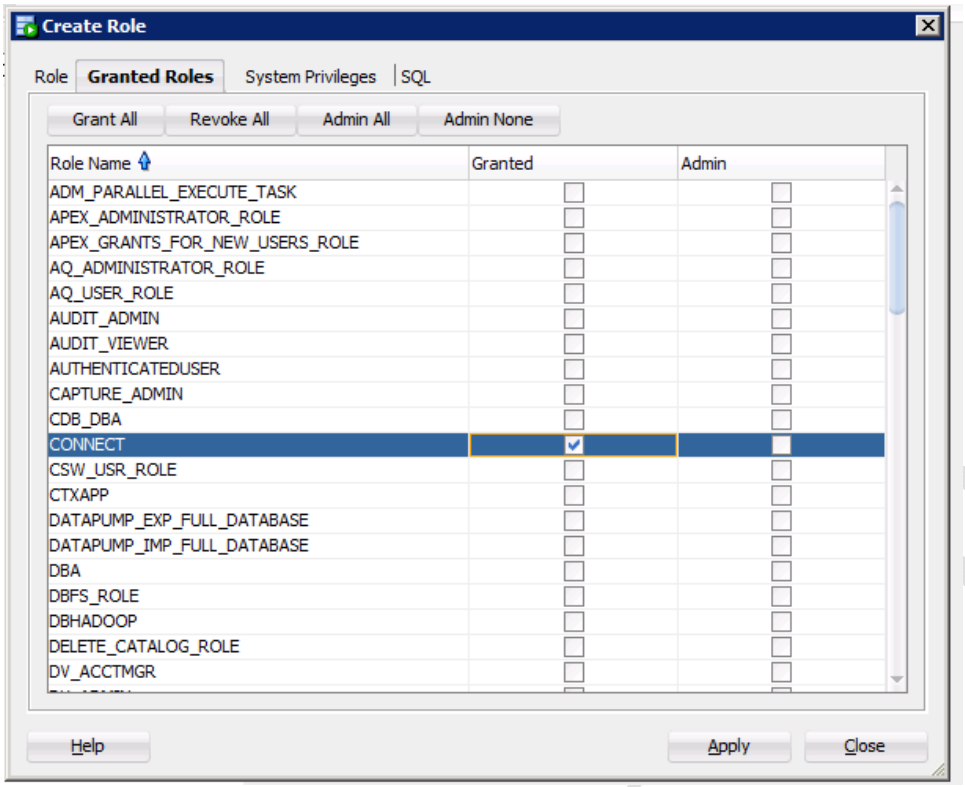
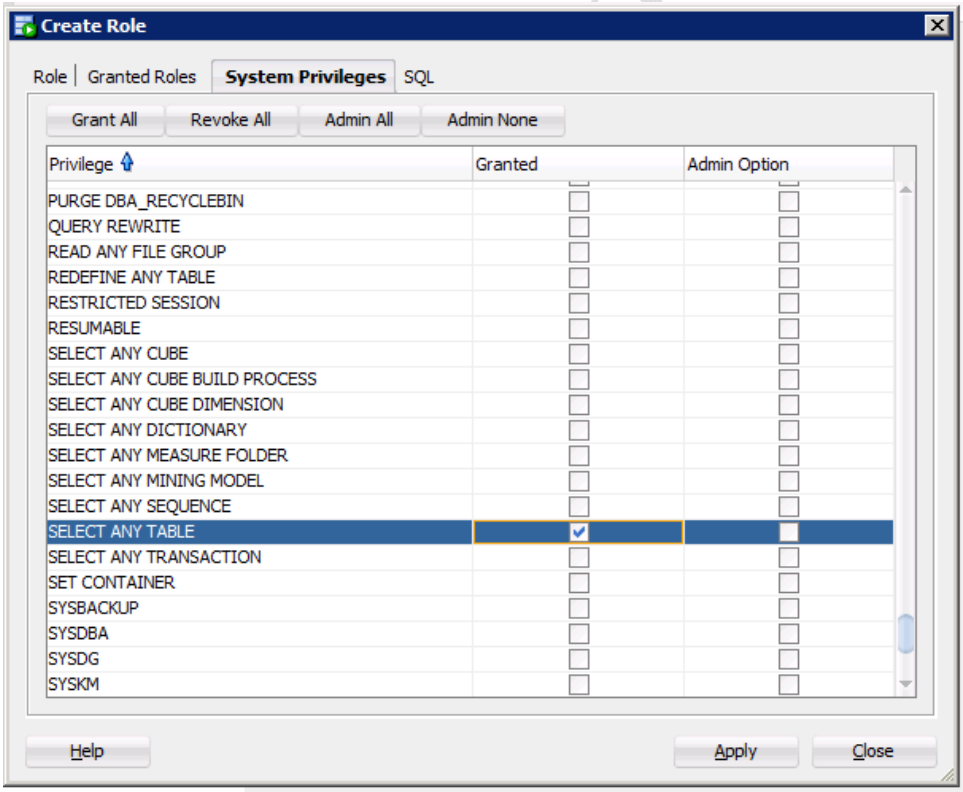


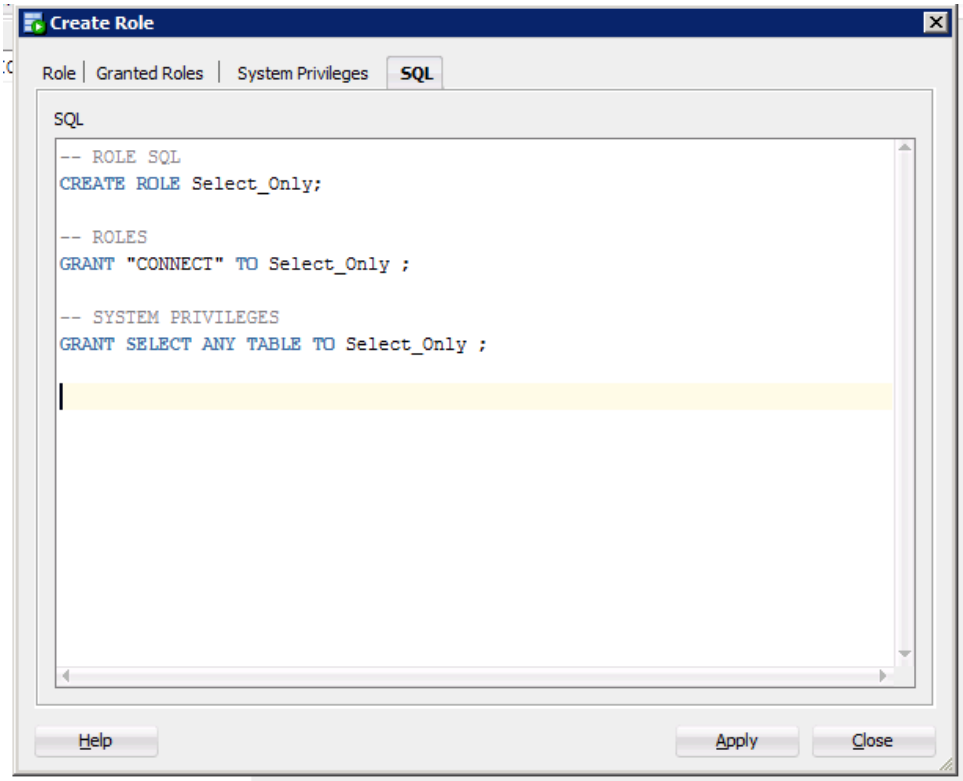
Figure 88. Screenshot. Simple user edits in SQL Developer.

Managing Roles

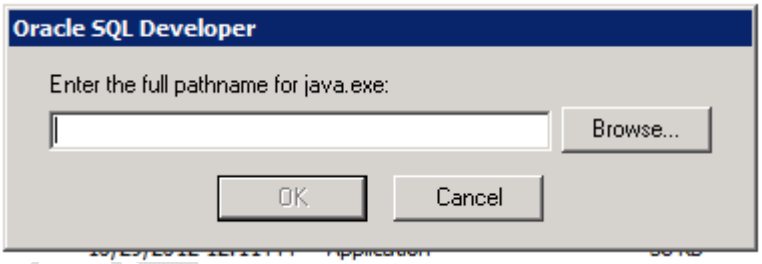


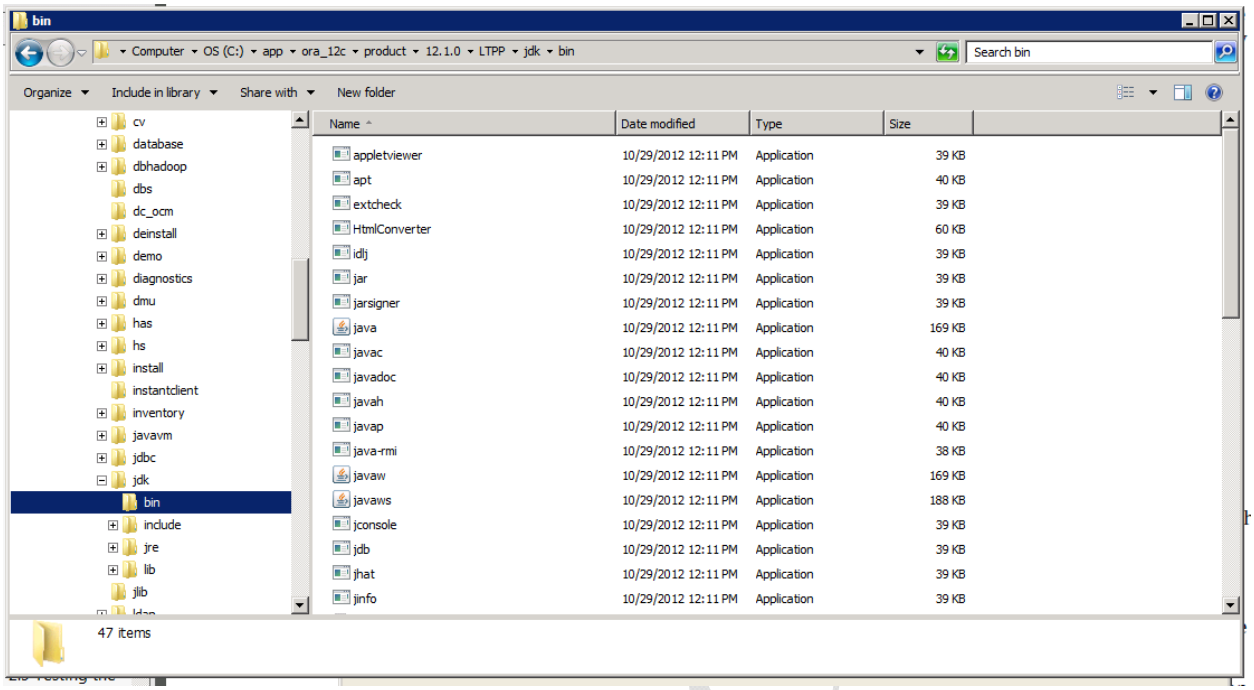

Create Role
Role
Granted Roles
System Privileges
SQL
Grant All
Revoke All
Admin All
Admin None
Role Name
Granted
Admin
ADM_PARALLEL_EXECUTE_TASK
APEX_ADMINISTRATOR_ROLE
APEX_GRANTS_FOR_NEW_USERS_ROLE
AQ_ADMINISTRATOR_ROLE
AQ_USER_ROLE
AUDIT_ADMIN
AUDIT_VIEWER
AUTHENTICATEDUSER
CAPTURE_ADMIN
CDB_DBA
CONNECT
CSW_USR_ROLE
CTXAPP
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE
DBA
DBFS_ROLE
DBHADOOP
DELETE_CATALOG_ROLE
DV_ACCTMGR
Help
Apply
Close

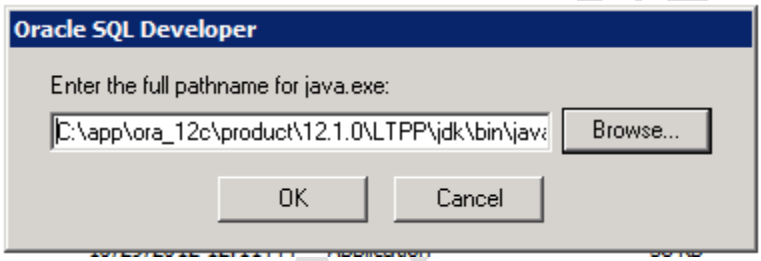

Create Role
Role
Granted Roles
System Privileges
SQL
Grant All
Revoke All
Admin All
Admin None
Privilege
Granted
Admin Option
PURGE DBA_RECYCLEBIN
QUERY REWRITE
READ ANY FILE GROUP
REDEFINE ANY TABLE
RESTRICTED SESSION
RESUMABLE
SELECT ANY CUBE
SELECT ANY CUBE BUILD PROCESS
SELECT ANY CUBE DIMENSION
SELECT ANY DICTIONARY
SELECT ANY MEASURE FOLDER
SELECT ANY MINING MODEL
SELECT ANY SEQUENCE
SELECT ANY TABLE
SELECT ANY TRANSACTION
SET CONTAINER
SYSBACKUP
SYSDBA
SYSDG
SYSKM
Help
Apply
Close

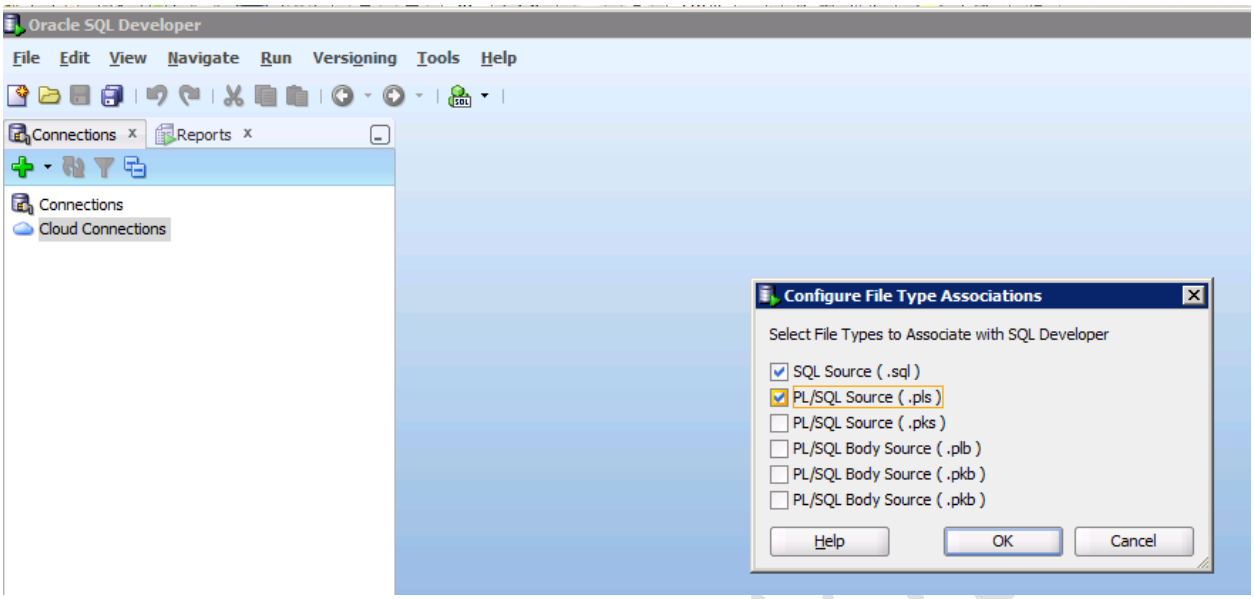


INSTALLING SQL DEVELOPER

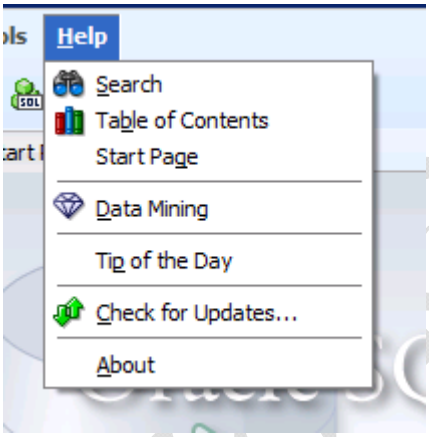



bin
Computer ▸ OS (C:) ▸ app ▸ ora_12c ▸ product ▸ 12.1.0 ▸ LTPP ▸ jdk ▸ bin
Search bin
Organize
Include in library
Share with
New folder
cv
database
dbhadoop
dbs
dc_ocm
deinstall
demo
diagnostics
dmu
has
hs
install
instantclient
inventory
javavm
jdbc
jdk
bin
include
jre
lib
jlib
Name
Date modified
Type
Size
appletviewer 10/29/2012 12:11 PM Application 39 KB
apt 10/29/2012 12:11 PM Application 40 KB
extcheck 10/29/2012 12:11 PM Application 39 KB
HtmlConverter 10/29/2012 12:11 PM Application 60 KB
idlj 10/29/2012 12:11 PM Application 39 KB
jar 10/29/2012 12:11 PM Application 39 KB
jarsigner 10/29/2012 12:11 PM Application 39 KB
java 10/29/2012 12:11 PM Application 169 KB
javac 10/29/2012 12:11 PM Application 40 KB
javadoc 10/29/2012 12:11 PM Application 40 KB
javah 10/29/2012 12:11 PM Application 40 KB
javap 10/29/2012 12:11 PM Application 40 KB
java-rmi 10/29/2012 12:11 PM Application 38 KB
javaw 10/29/2012 12:11 PM Application 169 KB
javaws 10/29/2012 12:11 PM Application 188 KB
jconsole 10/29/2012 12:11 PM Application 39 KB
jdb 10/29/2012 12:11 PM Application 39 KB
jhat 10/29/2012 12:11 PM Application 39 KB
jinfo 10/29/2012 12:11 PM Application 39 KB
47 items


Oracle SQL Developer
Enter the full pathname for java.exe:
C:\app\ora_12c\product\12.1.0\LTPP\jdk\bin\java
Browse...
OK
Cancel



Update SQL Developer from Help



OI

APPENDIX N. SOFTWARE APPLICATIONS

The server was delivered with the Windows Server 2008 R2 Operating System. *This was then configured to comply with NIST 800-53 Revision 2 Annex 1 since this is a low impact system.*

After configuration, anti-virus software was installed. The applications installed were Oracle 12c, Oracle 11g Client, Symantec Backup and various utilities. Once Oracle was installed, the production database instance, IMSProd was created. Then IMSTest and IMSDev were cloned.

The following is a list of software on the central server.

Software	**Renewal Date**	**Renewed by**
Symantec Backup Exec 2015 (maintenance)	Jan-2017	FHWA
Oracle 12c	N/A	DOT*
SQLDeveloper 4.x	Freeware	
Winzip 19	Indefinite	DOT
Adobe Acrobat ?	N/A	DOT
TextPad	Shareware	
Notepad++	Freeware	
PowerDesk 9	Indefinite	LTPP

*Team Leader and COR have licensing information

On at least a monthly basis the server should be connected to the Internet for operating system and anti-virus software updates. Use the Windows Update service to keep the operating system current on patches. Use Symantec Live Update for updates to the anti-virus and back up software. Patching of the Oracle software is done in coordination with patches to the DPW.

OPERATING SYSTEM

Operating system updates can also applied as individual patches downloaded from Microsoft on a separate computer. These patches are located by going to http://www.microsoft.com/technet/security/current.aspx and performing a Microsoft Security Bulletin Search. We are interested in searching for all bulletins for Windows Server 2008 x64 SP2. An example search is shown below, in **Figure 89**.

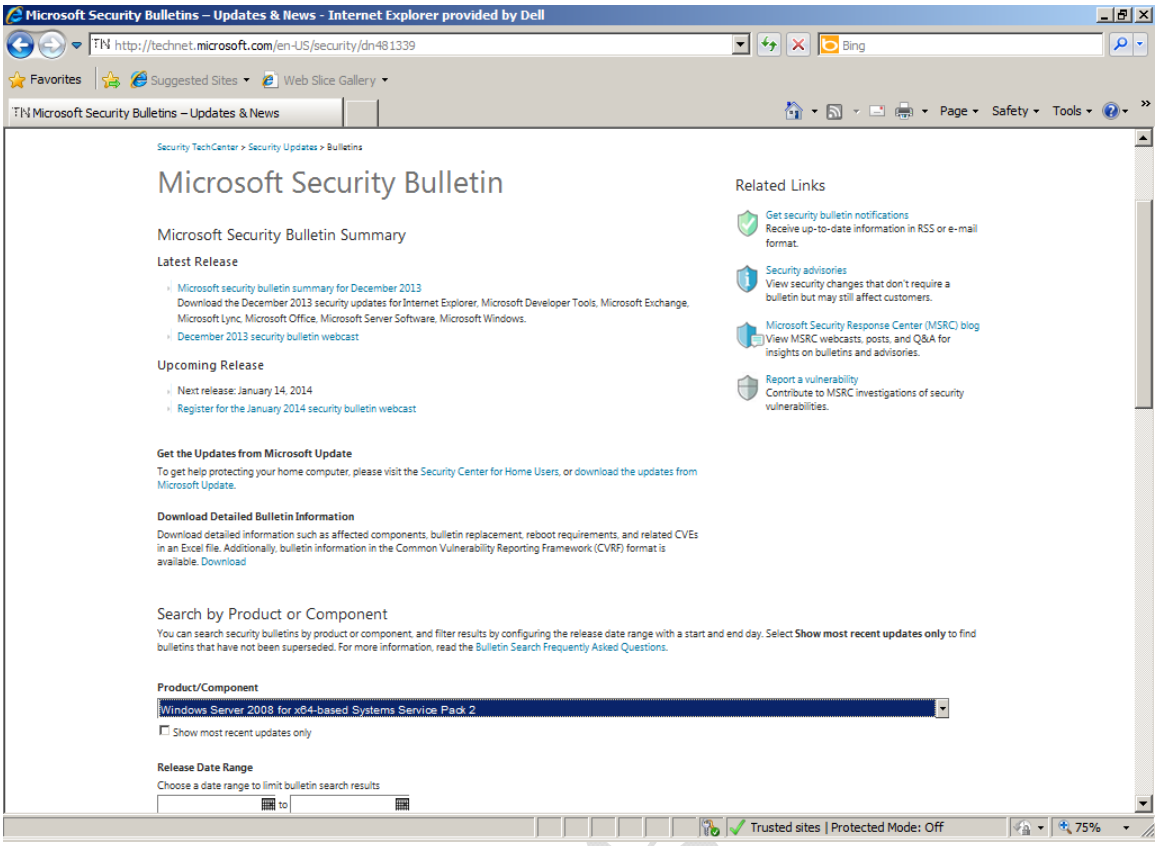


Figure 89. Screenshot. Example search for OS updates

Each patch that has not been applied is downloaded to a flash drive or other portable media. The media containing the patches is then mounted on the server and the patches are applied while logged in as an administrator.

- ***Operating System Updates***

Operating system updates are applied as individual patches downloaded from Microsoft on a separate computer since internet access is not available from the server. These patches are located by going to https://technet.microsoft.com/en-us/security/bulletin

and performing a Microsoft Security Bulletin Search. We are interested in searching for all bulletins for Windows Server 2008 SP2. An example search is shown in **Figure 90**.

0

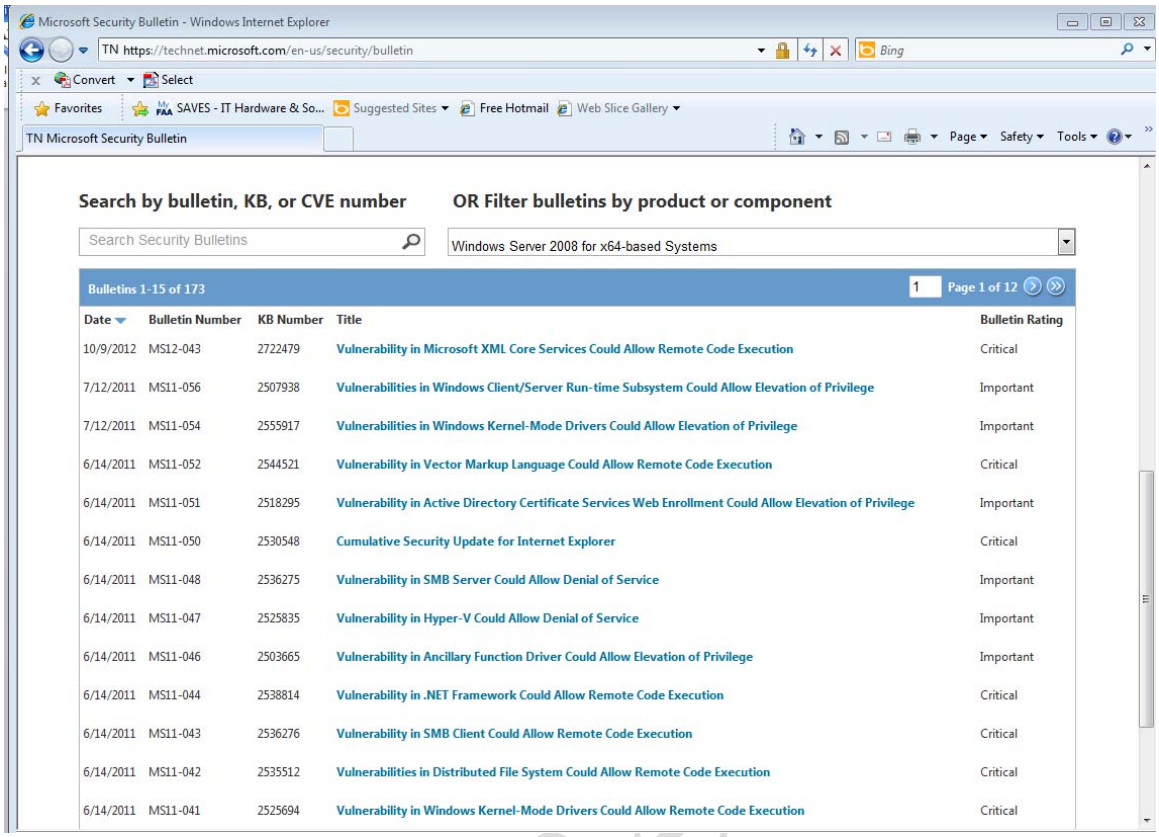


Figure 90. Screenshot. Example search for OS updates

Each patch that has not been applied is downloaded to a flash drive or other portable media. The media containing the patches is then mounted on the server and the patches are applied while logged in as an administrator.

ORACLE

Oracle patches can be found using My Oracle Support (https://support.oracle.com.)

Oracle patches can be downloaded http://www.oracle.com/technetwork/topics/security/alerts-086861.html from “My Oracle Support” formerly Metalink. The general procedure is to perform a knowledge base search for the update that you are interested in. For example, you could search for “Critical Patch Update July 2009 Oracle Products”. In the Patch Availability document, search for the table listing the critical patch update availability for Oracle Database. Then find the patch number for version 10.2.0.4 on Windows x86-64. In the example below, this is patch 8559467 (see **Figure 91**).

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

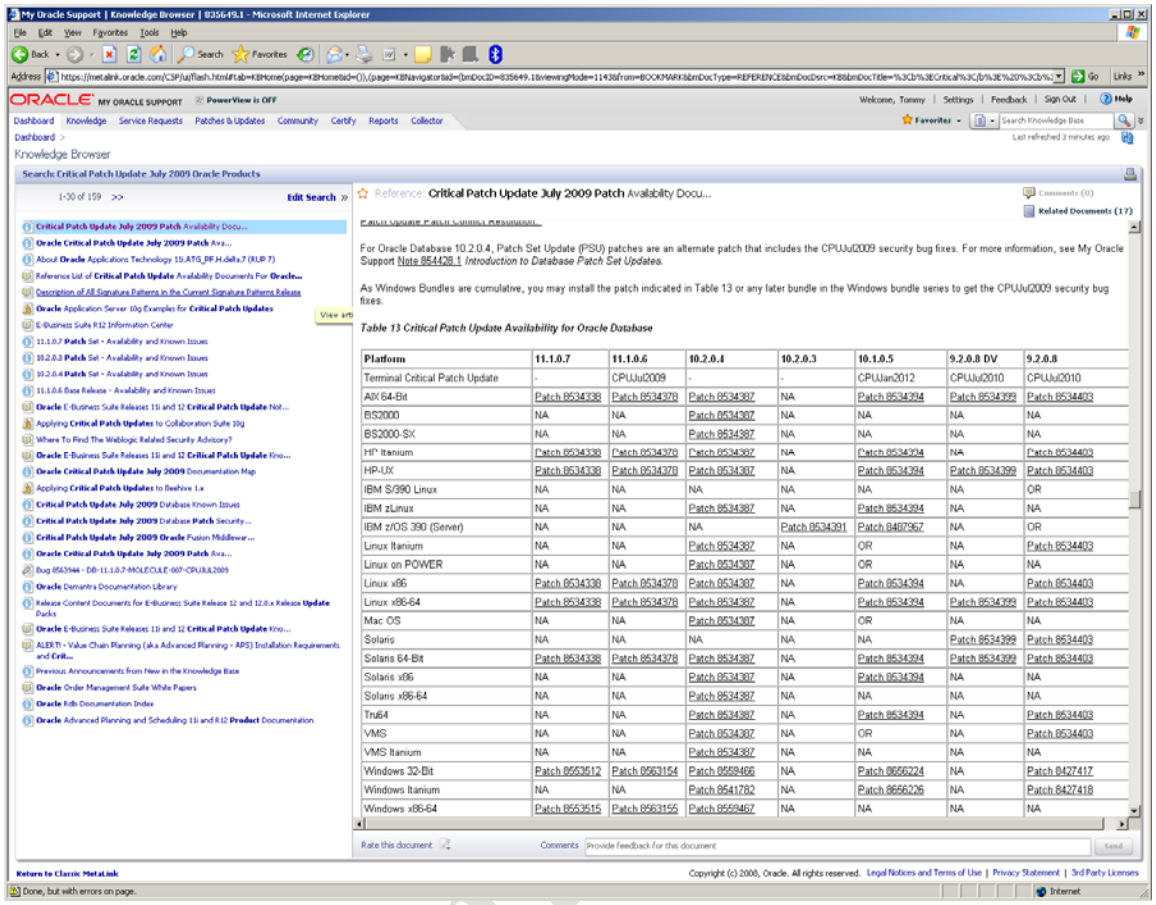


Figure 91. Screenshot. Example search for Oracle update

After locating the patch number, you proceed to the “Patches & Updates” tab and select a simple search. Enter the patch number that you found in the table and hit “Go” (see **Figure 92**).

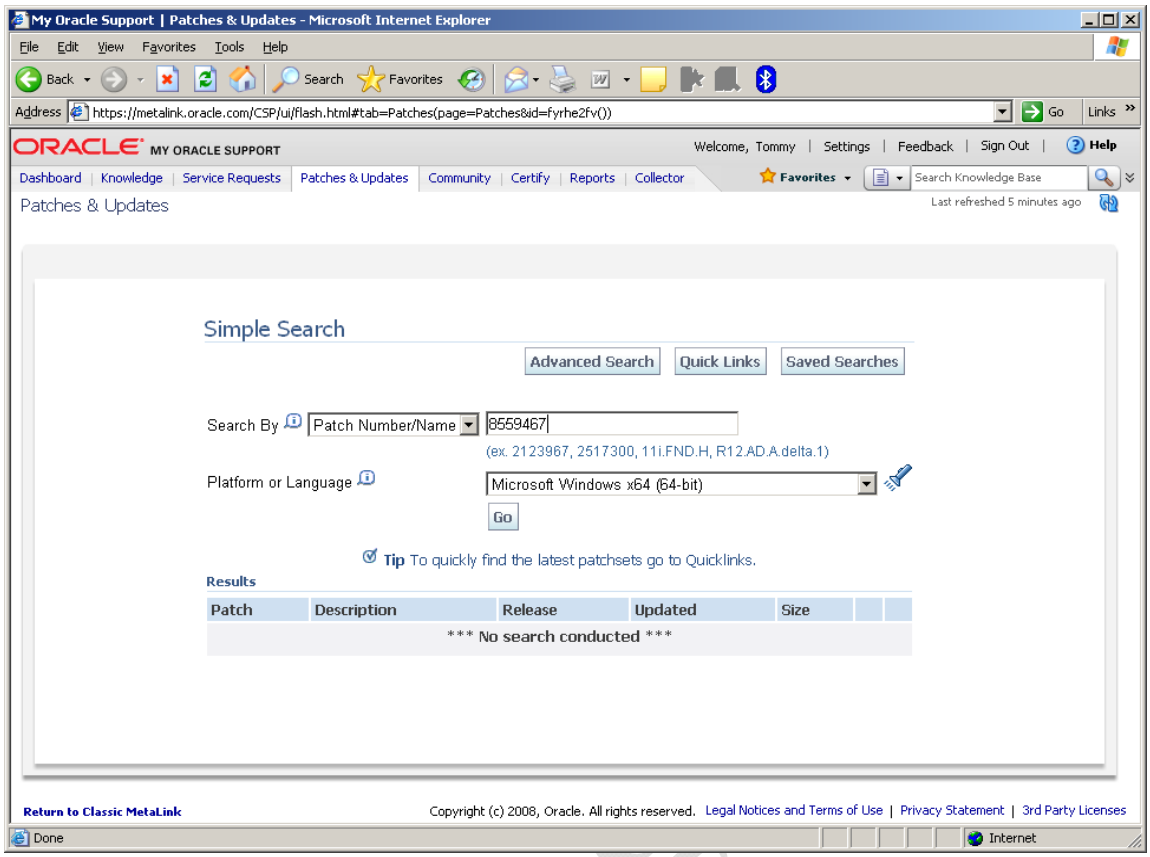


Figure 92. Screenshot. Oracle Patches & Updates – Simple Search Window

That will bring you to the actual download screen (see **Figure 93**).

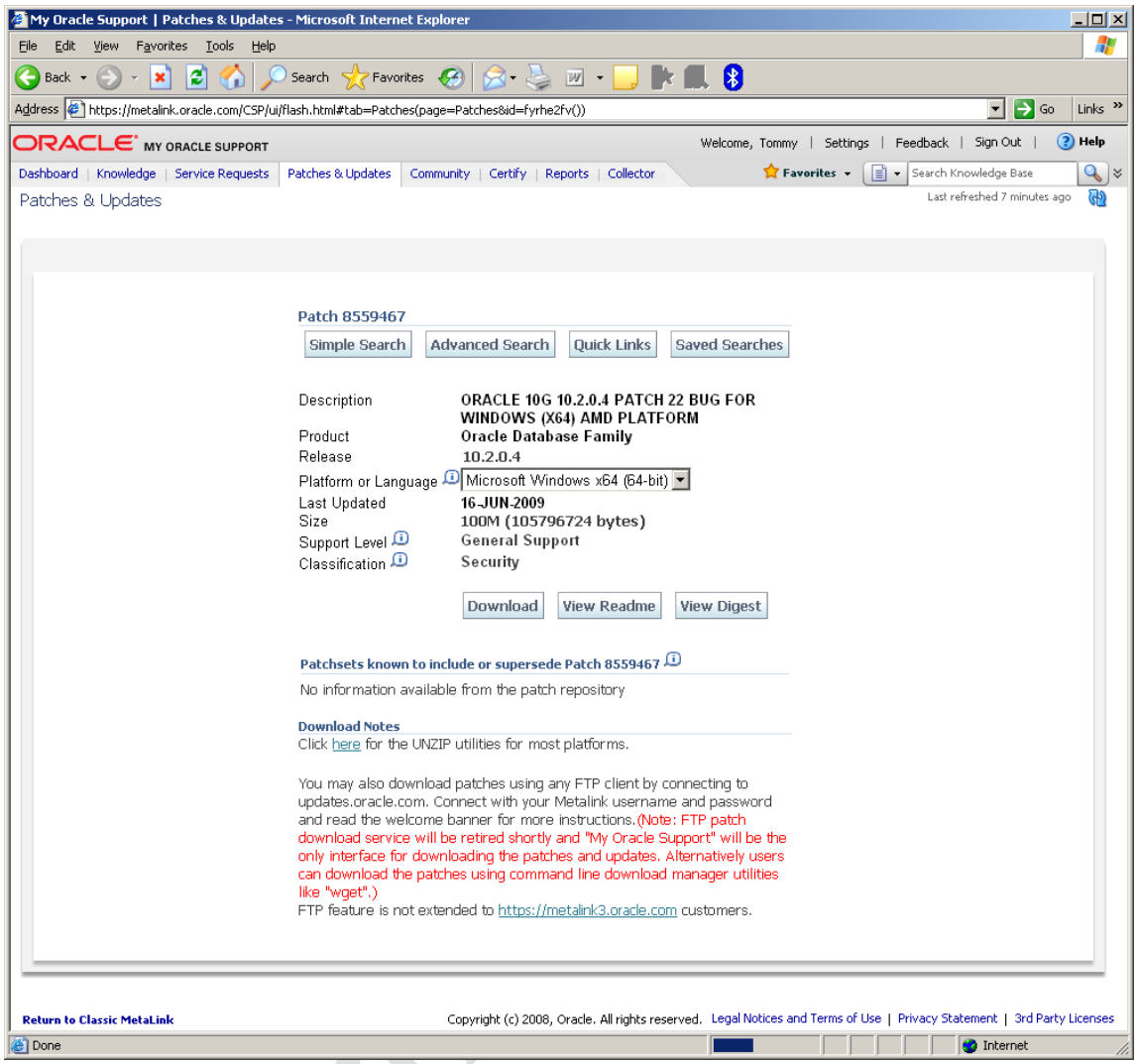


Figure 93. Screenshot. Oracle Patches & Updates - Patch 8559467 Download Window

Be sure to view the readme file. It will tell which version of OPatch is required to install this patch and other prerequisites. It will also give step by step instructions for installing the patch.

Oracle patches can be downloaded from “My Oracle Support” formerly Metalink. The general procedure is to perform a knowledge base search for the update that you are interested in. For example, you could search for “Critical Patch Update (CPU) July 2009 Oracle Products”. In the Patch Availability document, search for the table listing the critical patch update availability for Oracle Database. Then find the patch number for version 10.2.0.3 on Windows 32-Bit. In the example below (**Figure 94**), you will notice that the patch is listed as N/A. This is because support for 10.2.0.3 ended on February 22,

2009. If you go back to the January 2009 Critical Patch Update, you will see that patch 7631965 is the last CPU available.

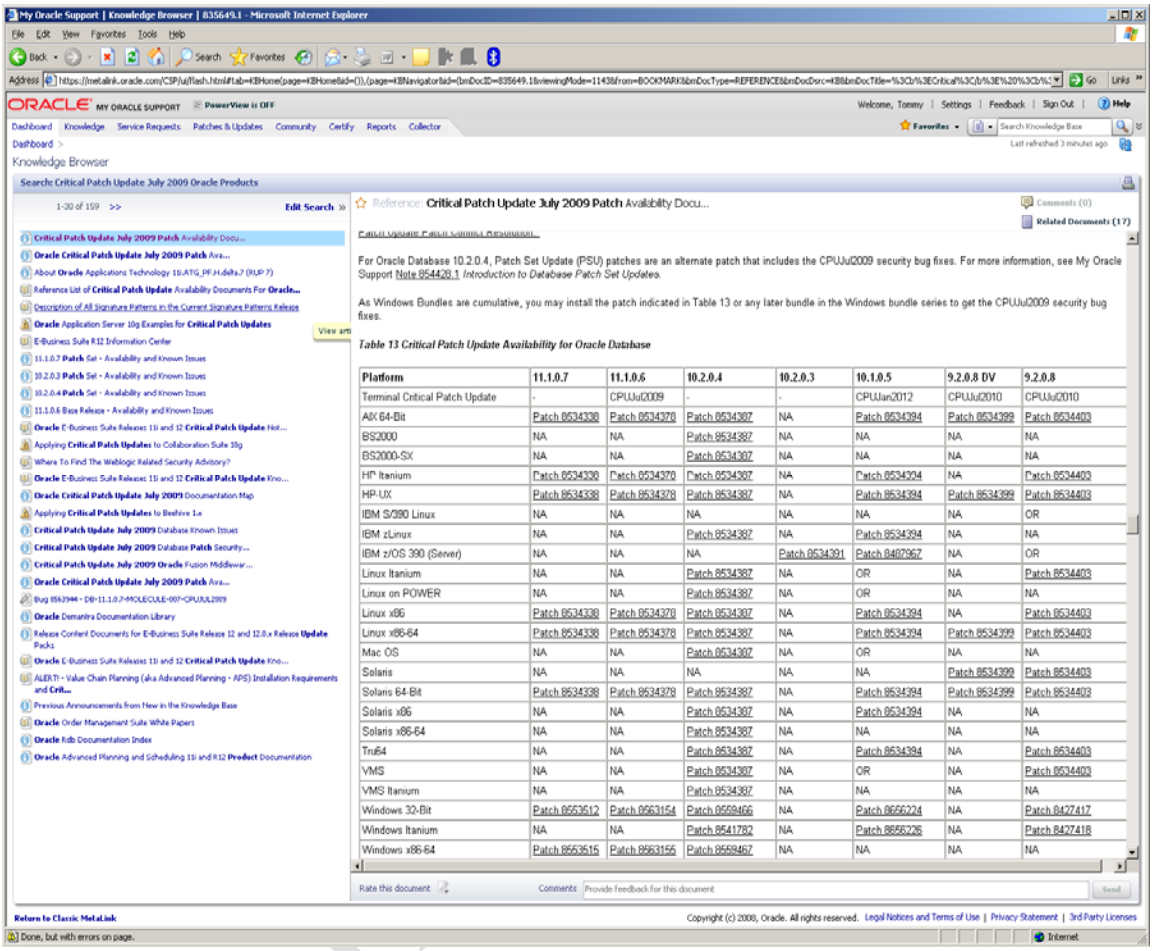


Figure 94. Screenshot. Example search for Oracle update

After locating the patch number, you proceed to the “Patches & Updates” tab and select a simple search. Enter the patch number that you found in the table and hit “Go” (see **Figure 95**).

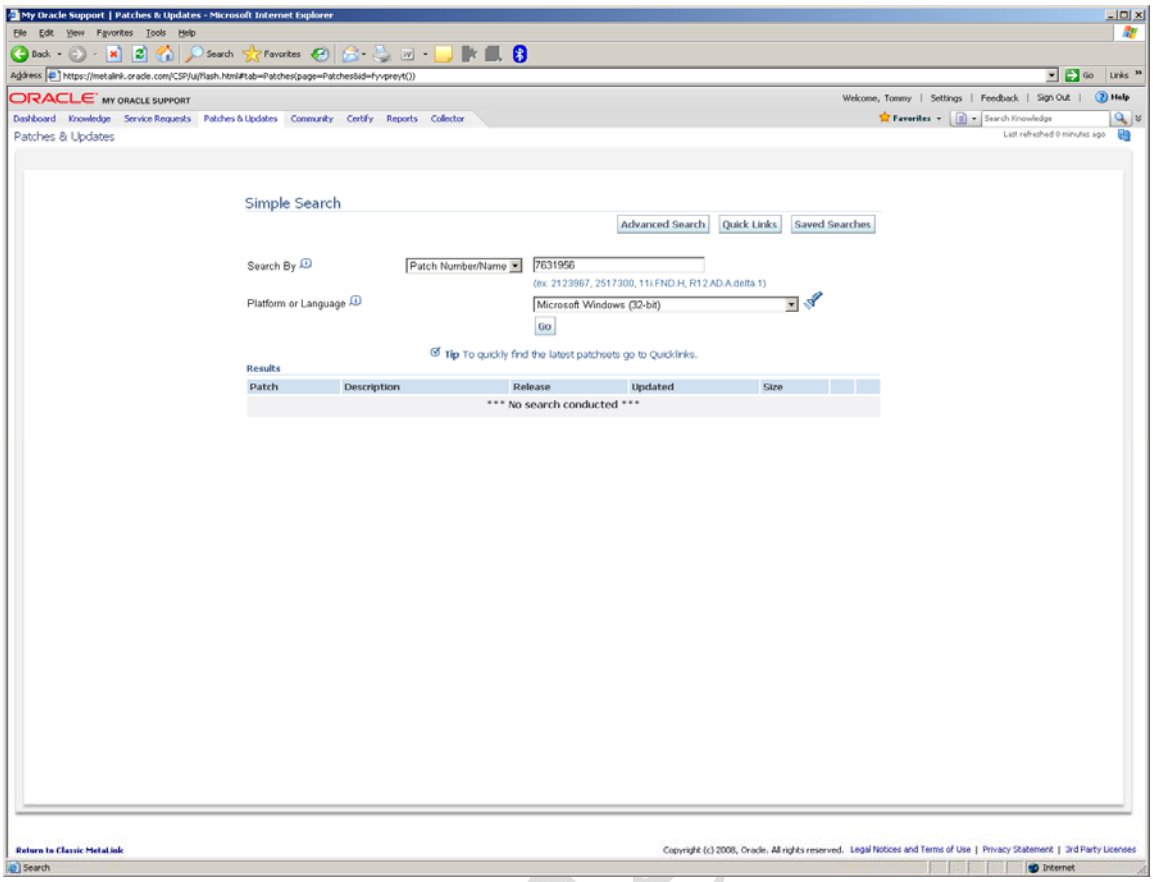


Figure 95. Screenshot.Oracle Patches & Updates - Simple Search Window

That will bring you to the actual download screen (**Figure 96**).

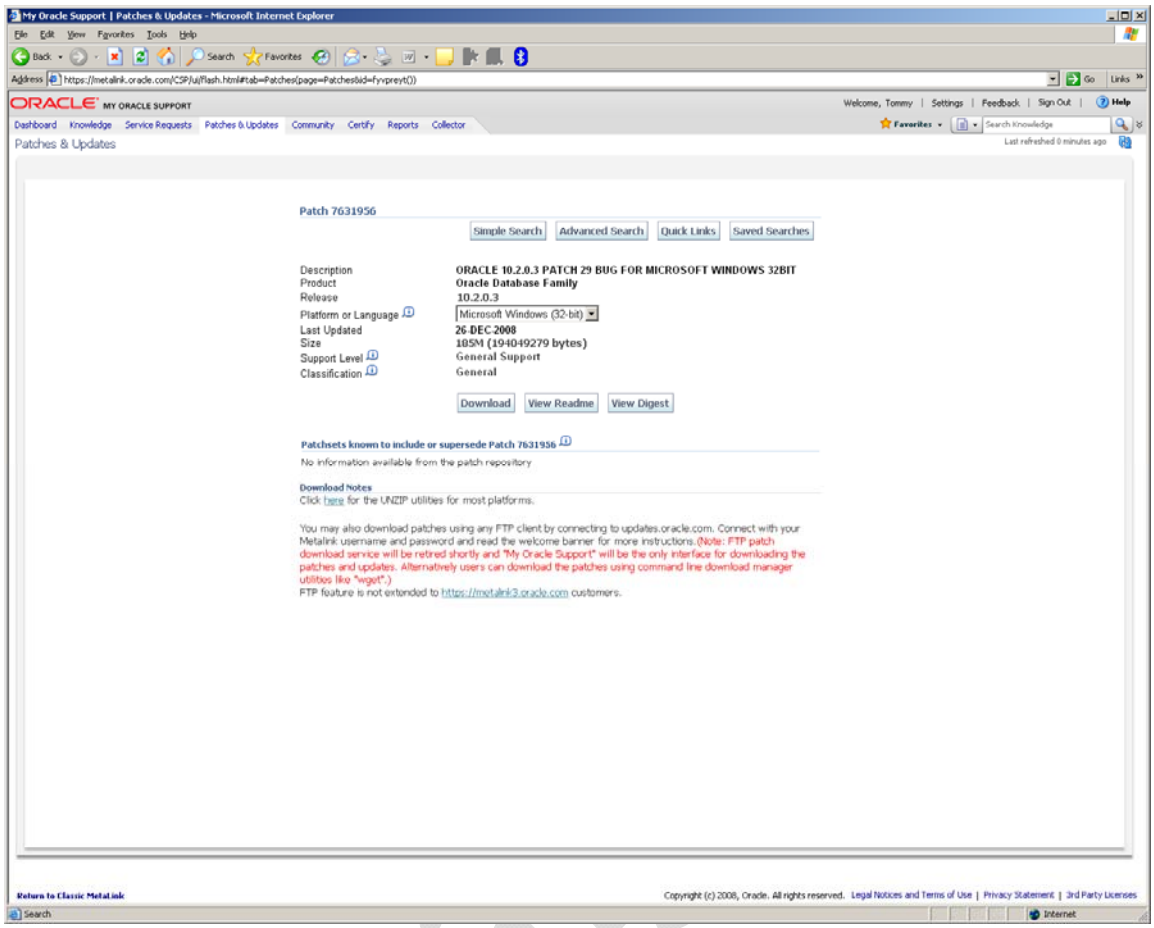


Figure 96. Screenshot. Oracle Patches & Updates - Patch 7631956 Download Window

You should be sure to view the readme file. It will tell you which version of OPatch is required to install this patch and other prerequisites. It will also give you step by step instructions for installing the patch.

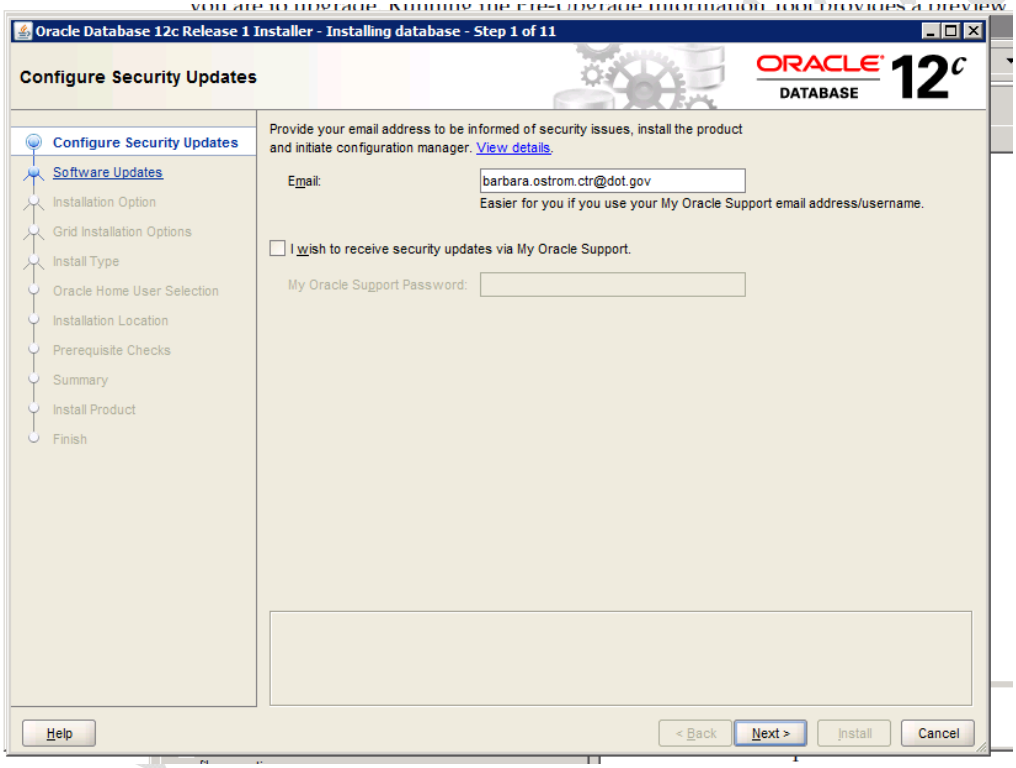
APPENDIX O. ORACLE INSTALLATION

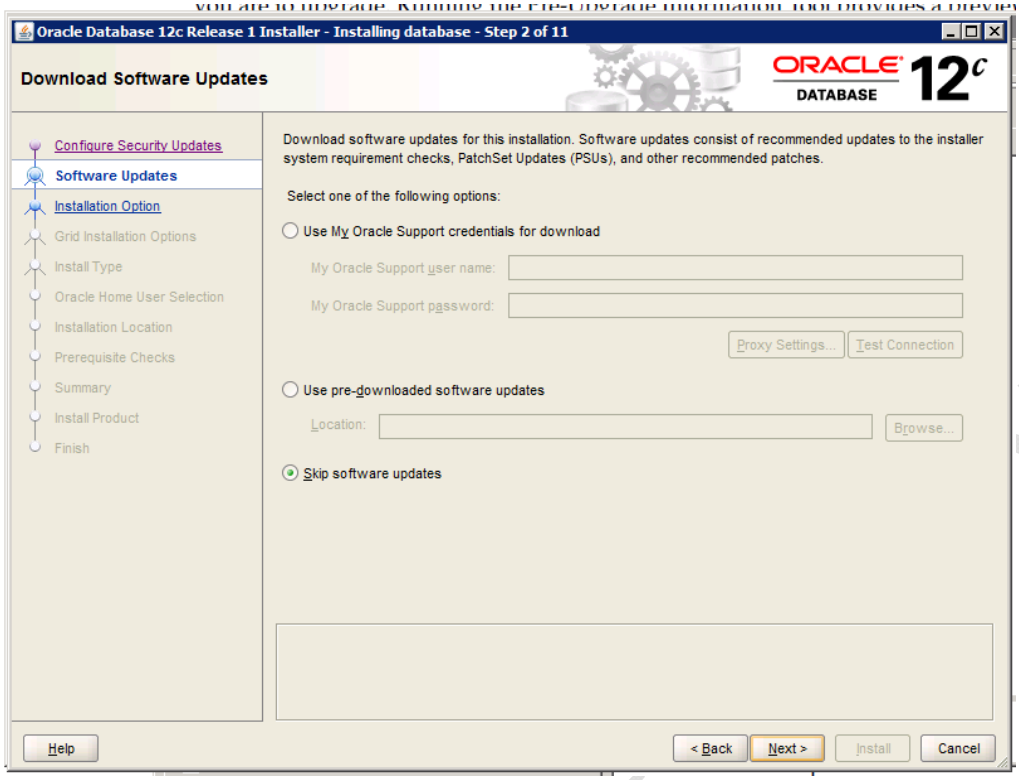
Oracle installation consists of two elements, installation of the Oracle software and the creation of the instances. Installation of Oracle to a new version occurs every 3 to 5 years as Oracle support expires for a named version or hardware is replaced. Creation of new instances typically occurs by cloning. Creation of special purpose instances or the original instance of a new version occurs much less frequently.

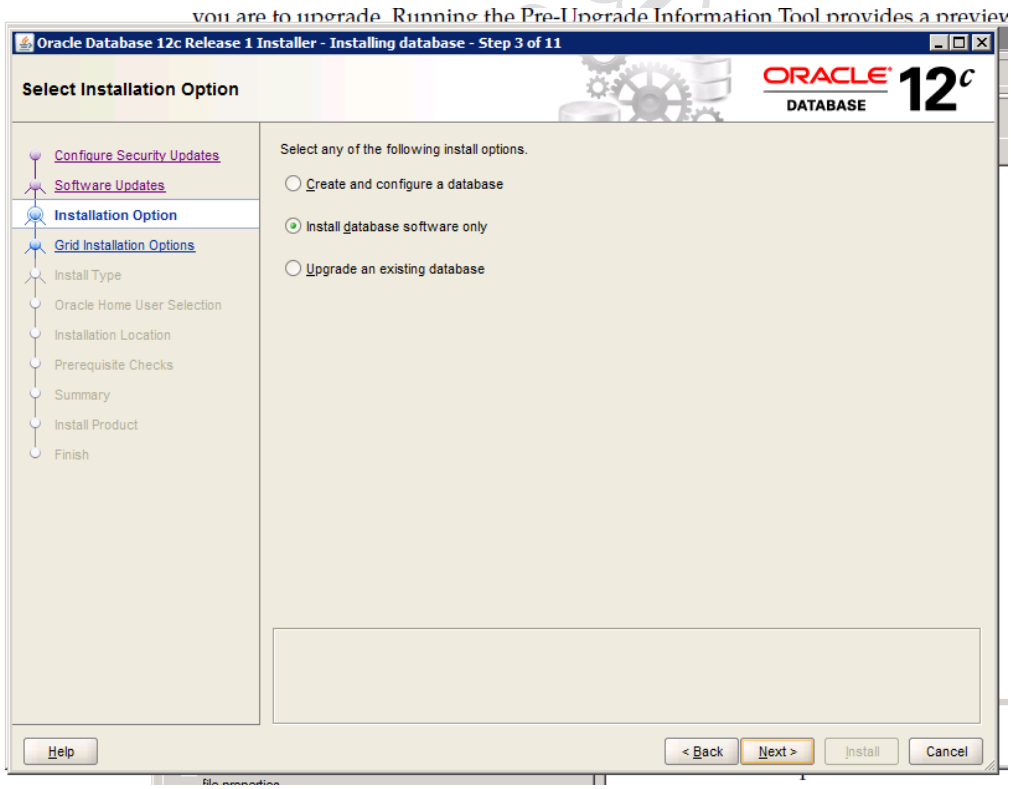
This section documents the installation process for version 12c and the process of creating an instance with tools available in it.

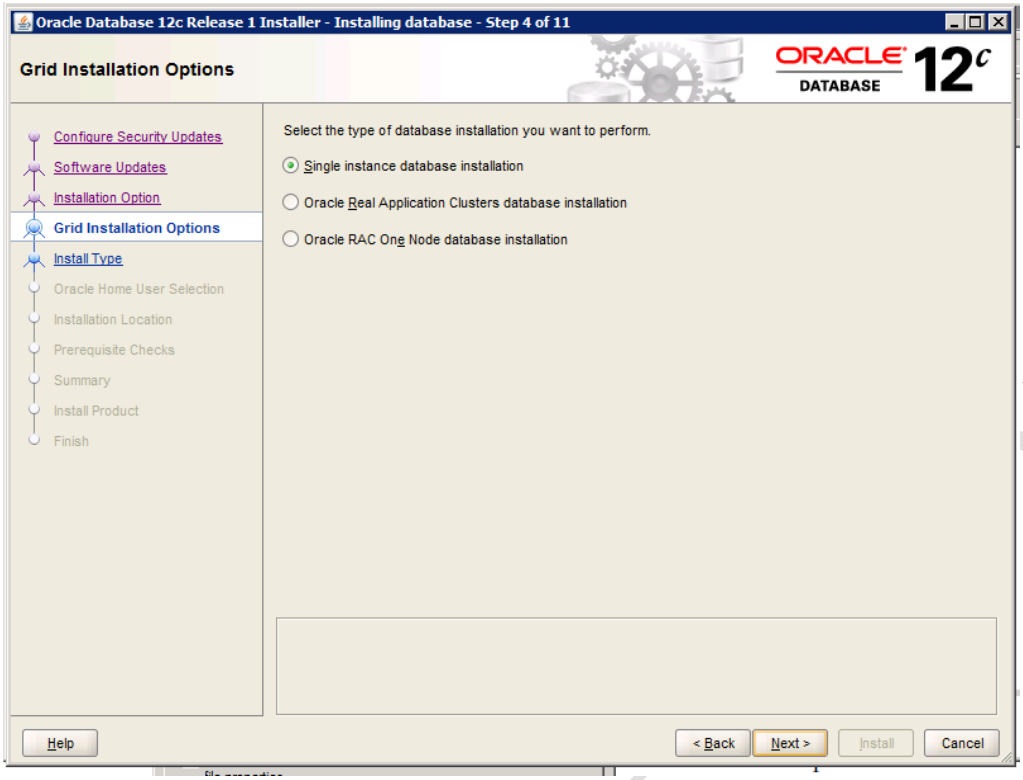
INSTALLING ORACLE 12C

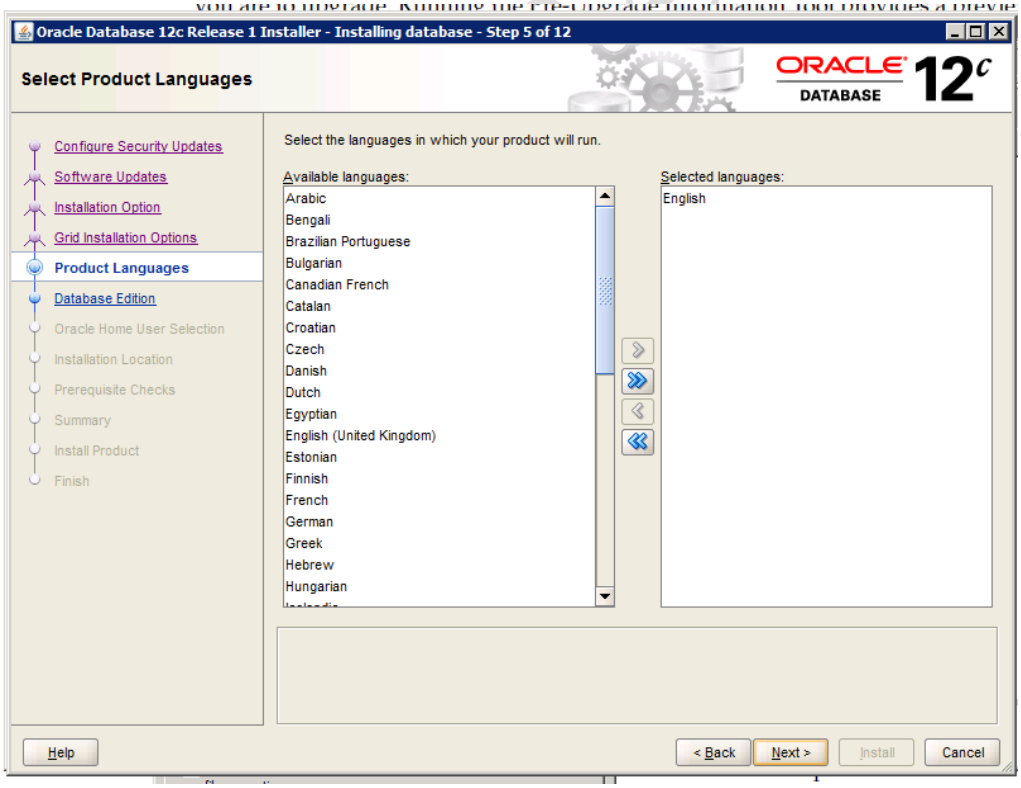
Oracle comes with a universal installer. Once the software is downloaded and unzipped to a working directory, clicking on the setup application begins the process.

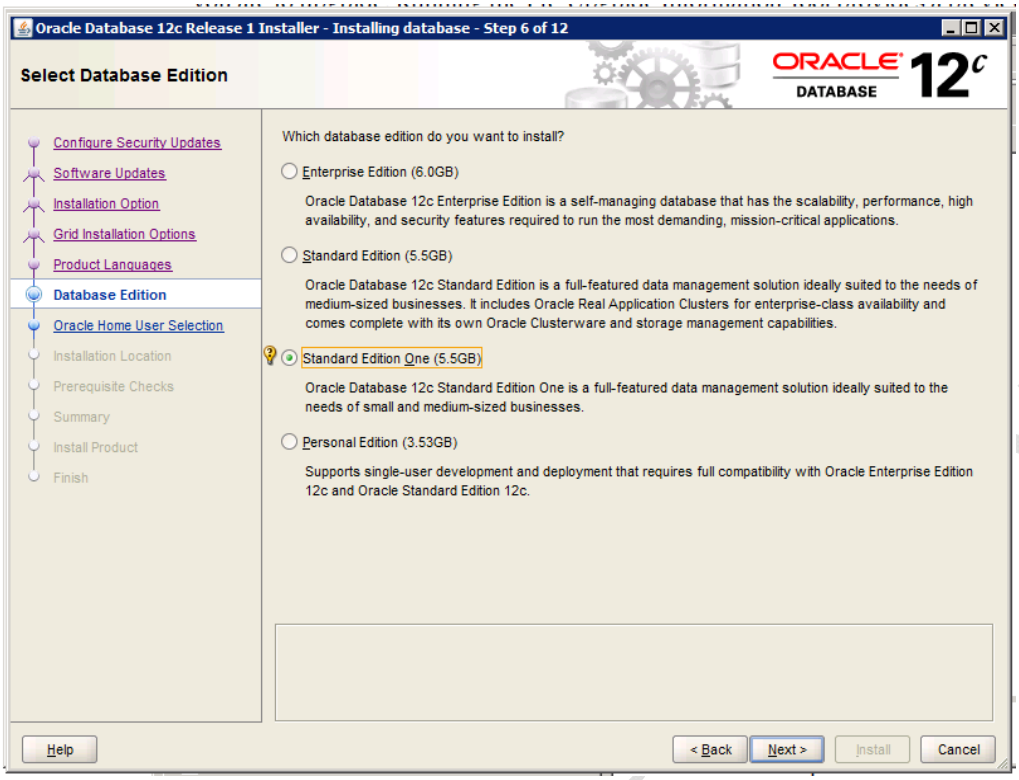


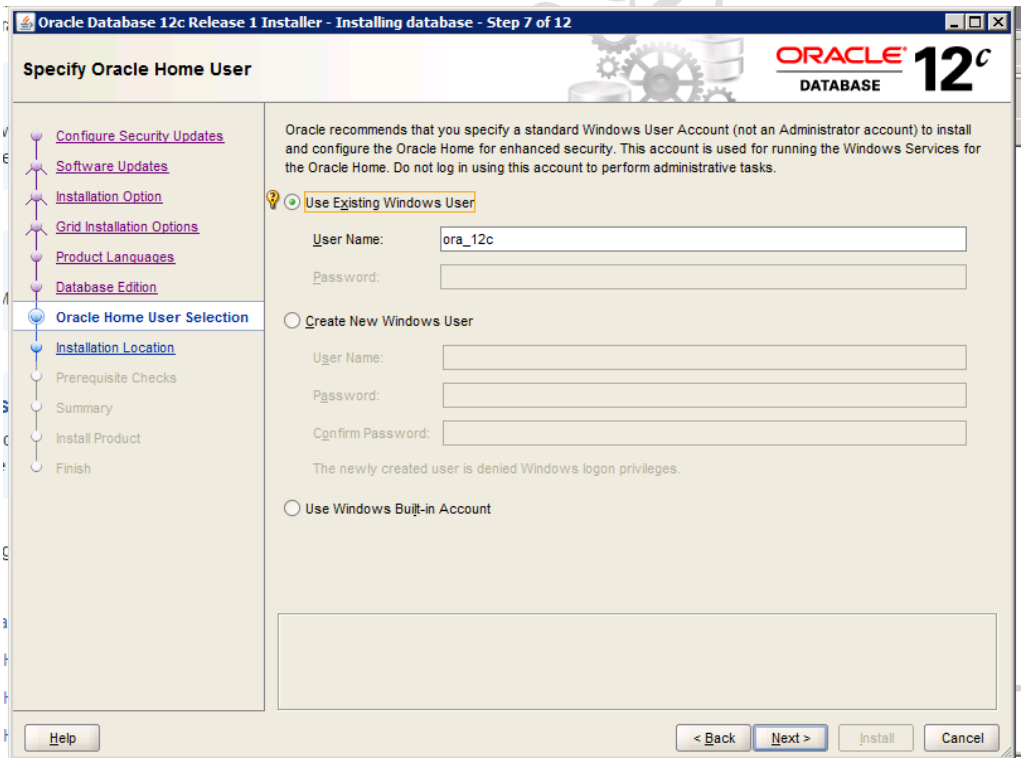

Oracle Database 12c Release 1 Installer - Installing database - Step 2 of 11
Download Software Updates
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Install Type
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Download software updates for this installation. Software updates consist of recommended updates to the installer system requirement checks, PatchSet Updates (PSUs), and other recommended patches.
Select one of the following options:
Use My Oracle Support credentials for download
My Oracle Support user name:
My Oracle Support password:
Proxy Settings...
Test Connection
Use pre-downloaded software updates
Location:
Browse...
Skip software updates
Help
< Back
Next >
Install
Cancel


Oracle Database 12c Release 1 Installer - Installing database - Step 3 of 11
Select Installation Option
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Install Type
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Select any of the following install options.
Create and configure a database
Install database software only
Upgrade an existing database
Help
< Back
Next >
Install
Cancel


Oracle Database 12c Release 1 Installer - Installing database - Step 4 of 11
Grid Installation Options
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Install Type
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Select the type of database installation you want to perform.
Single instance database installation
Oracle Real Application Clusters database installation
Oracle RAC One Node database installation
Help
< Back
Next >
Install
Cancel


Oracle Database 12c Release 1 Installer - Installing database - Step 5 of 12
Select Product Languages
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Product Languages
Database Edition
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Select the languages in which your product will run.
Available languages:
Arabic
Bengali
Brazilian Portuguese
Bulgarian
Canadian French
Catalan
Croatian
Czech
Danish
Dutch
Egyptian
English (United Kingdom)
Estonian
Finnish
French
German
Greek
Hebrew
Hungarian
Selected languages:
English
Help
< Back
Next >
Install
Cancel


Oracle Database 12c Release 1 Installer - Installing database - Step 6 of 12
Select Database Edition
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Product Languages
Database Edition
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Which database edition do you want to install?
Enterprise Edition (6.0GB)
Oracle Database 12c Enterprise Edition is a self-managing database that has the scalability, performance, high availability, and security features required to run the most demanding, mission-critical applications.
Standard Edition (5.5GB)
Oracle Database 12c Standard Edition is a full-featured data management solution ideally suited to the needs of medium-sized businesses. It includes Oracle Real Application Clusters for enterprise-class availability and comes complete with its own Oracle Clusterware and storage management capabilities.
Standard Edition One (5.5GB)
Oracle Database 12c Standard Edition One is a full-featured data management solution ideally suited to the needs of small and medium-sized businesses.
Personal Edition (3.53GB)
Supports single-user development and deployment that requires full compatibility with Oracle Enterprise Edition 12c and Oracle Standard Edition 12c.
Help
< Back
Next >
Install
Cancel

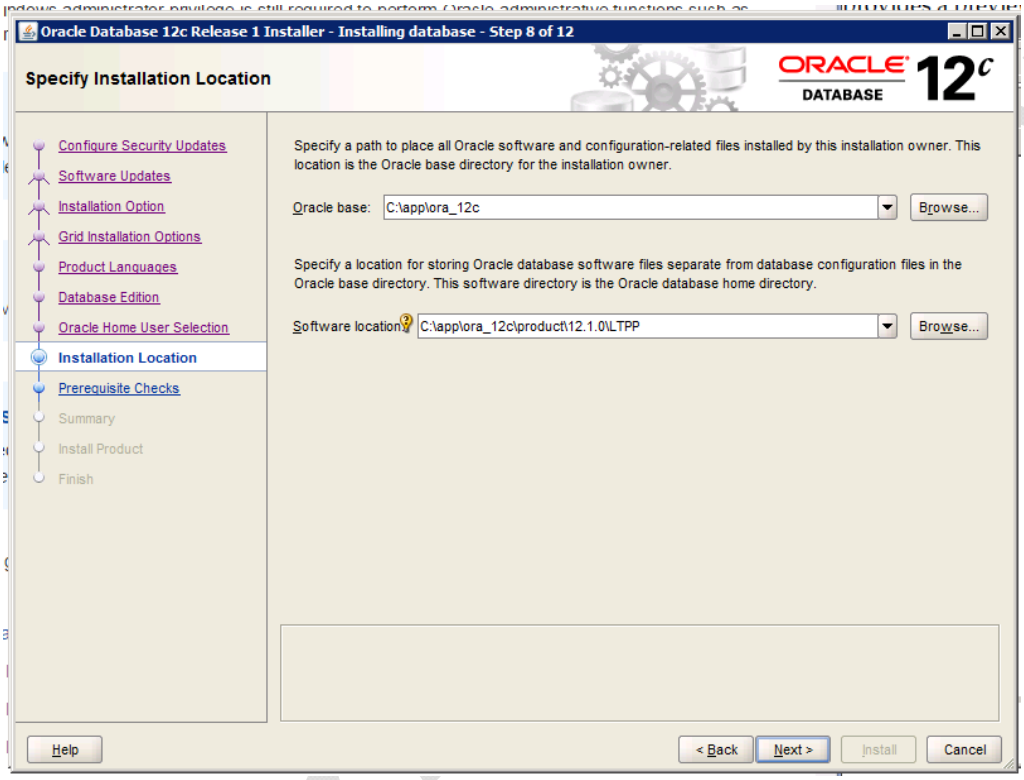

Oracle Database 12c Release 1 Installer - Installing database - Step 7 of 12
Specify Oracle Home User
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Product Languages
Database Edition
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Oracle recommends that you specify a standard Windows User Account (not an Administrator account) to install and configure the Oracle Home for enhanced security. This account is used for running the Windows Services for the Oracle Home. Do not log in using this account to perform administrative tasks.
Use Existing Windows User
User Name:
ora_12c
Password:
Create New Windows User
User Name:
Password:
Confirm Password:
The newly created user is denied Windows logon privileges.
Use Windows Built-in Account
Help
< Back
Next >
Install
Cancel

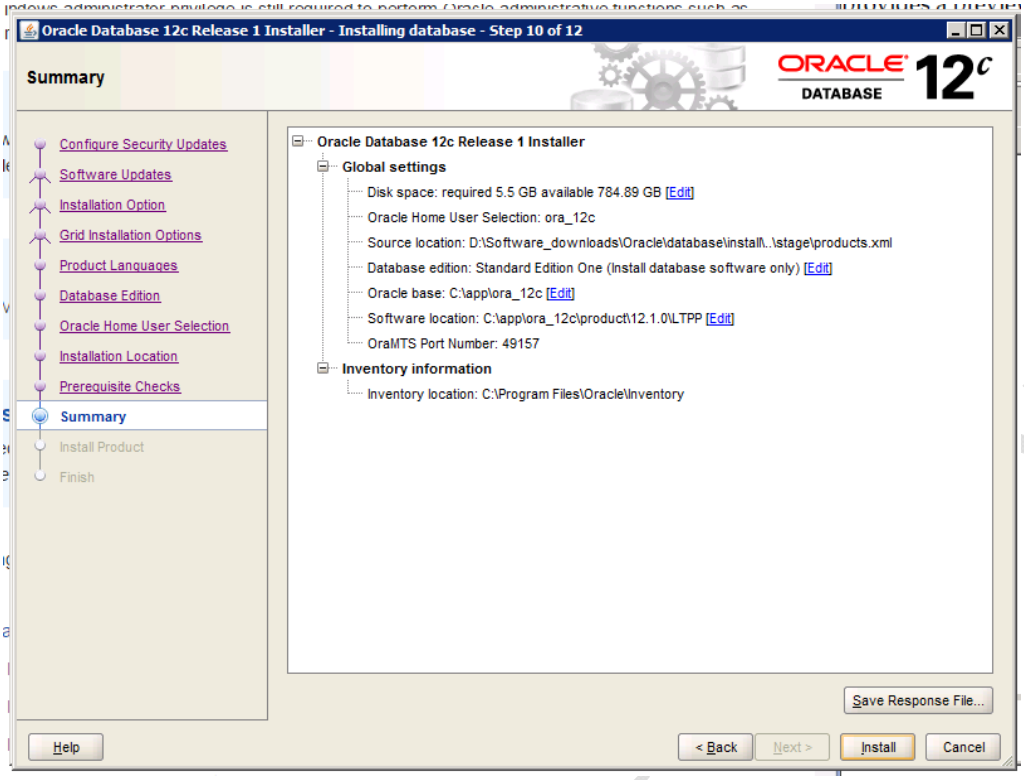
Info on Oracle Home User on Windows:

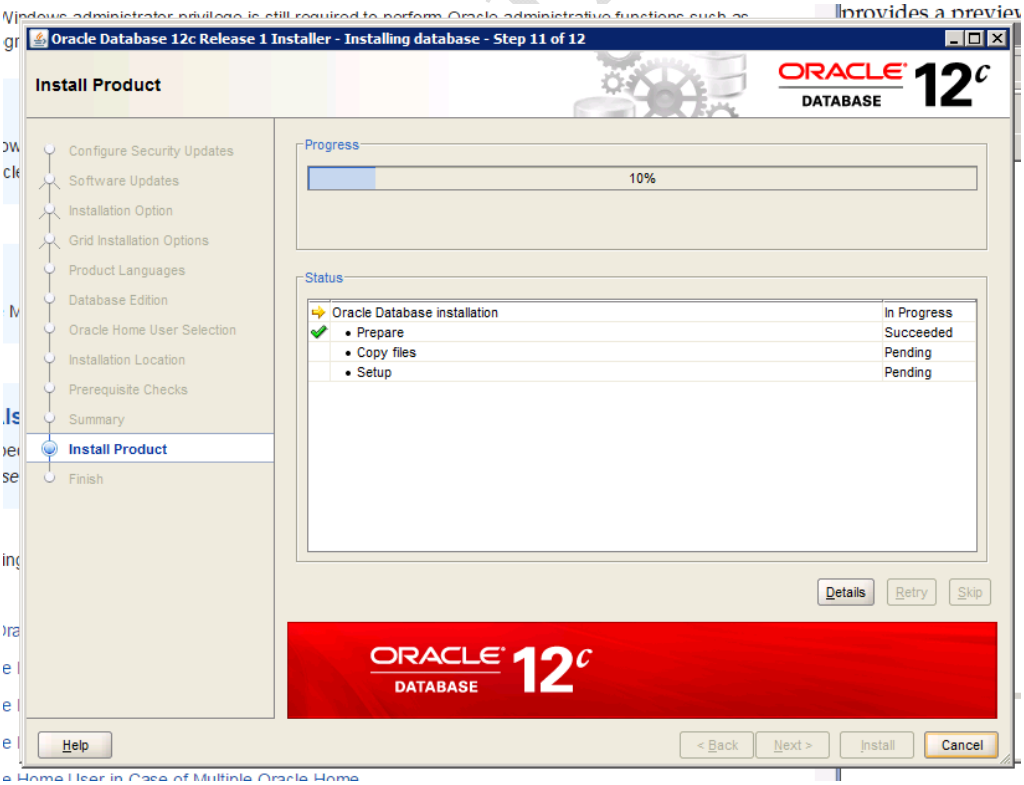
http://docs.oracle.com/database/121/NTQRF/oh_usr.htm

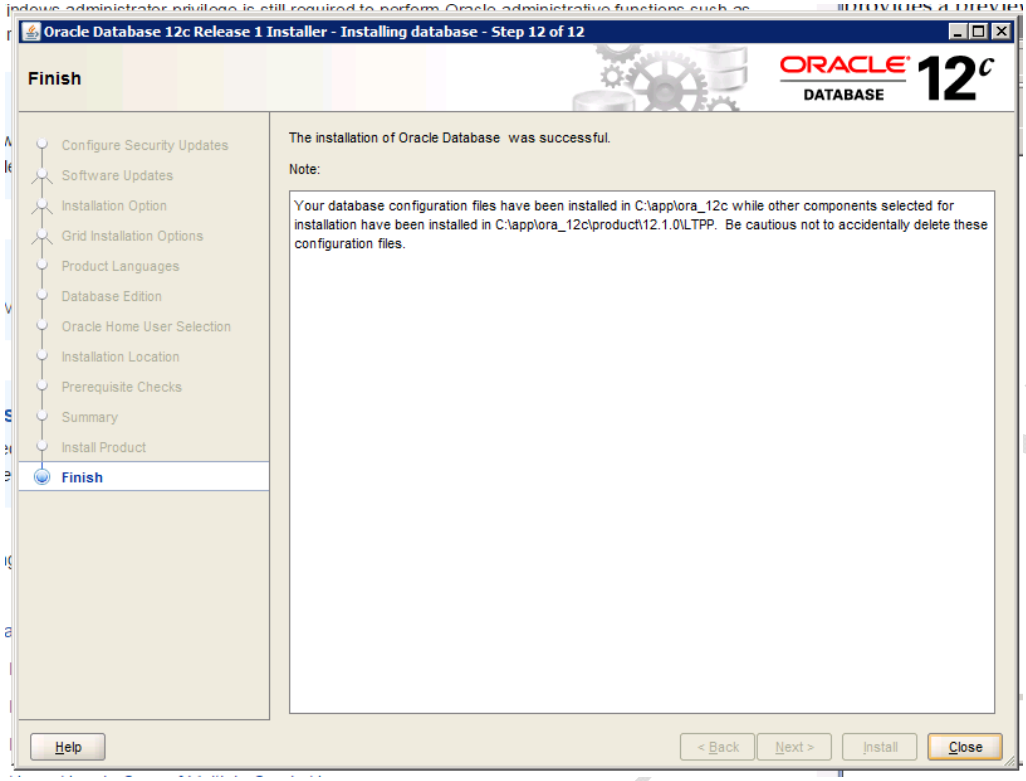
http://docs.oracle.com/database/121/NTDBI/install.htm#NTDBI0441

http://docs.oracle.com/database/121/NTQRF/oh_usr.htm#NTQRF673

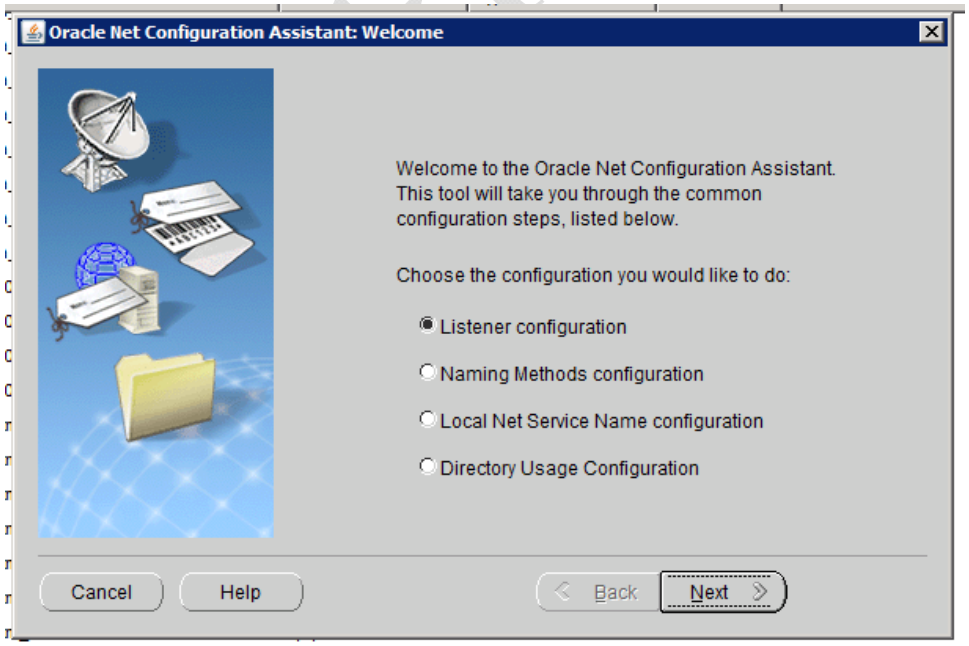


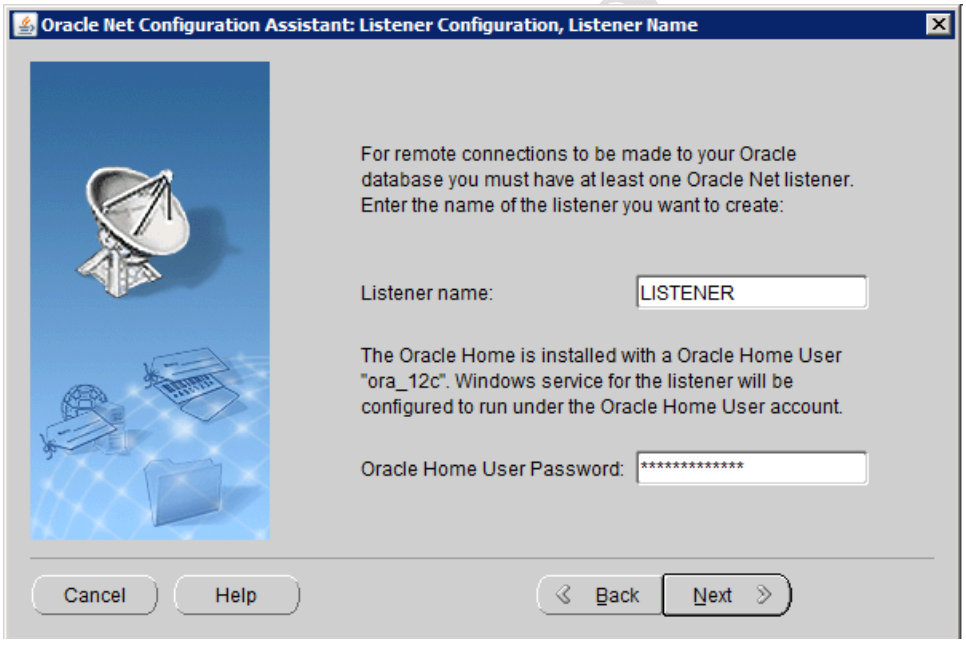

Oracle Database 12c Release 1 Installer - Installing database - Step 10 of 12
Summary
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Product Languages
Database Edition
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Oracle Database 12c Release 1 Installer
Global settings
Disk space: required 5.5 GB available 784.89 GB [Edit]
Oracle Home User Selection: ora_12c
Source location: D:\Software_downloads\Oracle\database\install\..\stage\products.xml
Database edition: Standard Edition One (Install database software only) [Edit]
Oracle base: C:\app\ora_12c [Edit]
Software location: C:\app\ora_12c\product\12.1.0\LTPP [Edit]
OraMTS Port Number: 49157
Inventory information
Inventory location: C:\Program Files\Oracle\Inventory
Save Response File...
Help
< Back
Next >
Install
Cancel

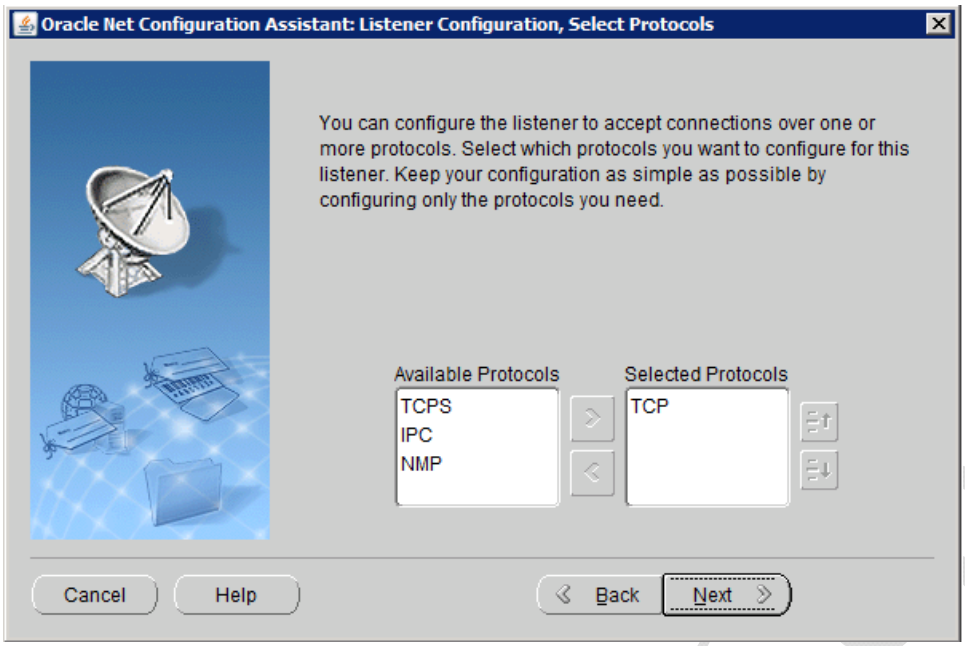

Oracle Database 12c Release 1 Installer - Installing database - Step 11 of 12
Install Product
ORACLE DATABASE 12c
Configure Security Updates
Software Updates
Installation Option
Grid Installation Options
Product Languages
Database Edition
Oracle Home User Selection
Installation Location
Prerequisite Checks
Summary
Install Product
Finish
Progress
10%
Status
Oracle Database installation
In Progress
Prepare
Succeeded
Copy files
Pending
Setup
Pending
Details
Retry
Skip
ORACLE DATABASE 12c
Help
< Back
Next >
Install
Cancel

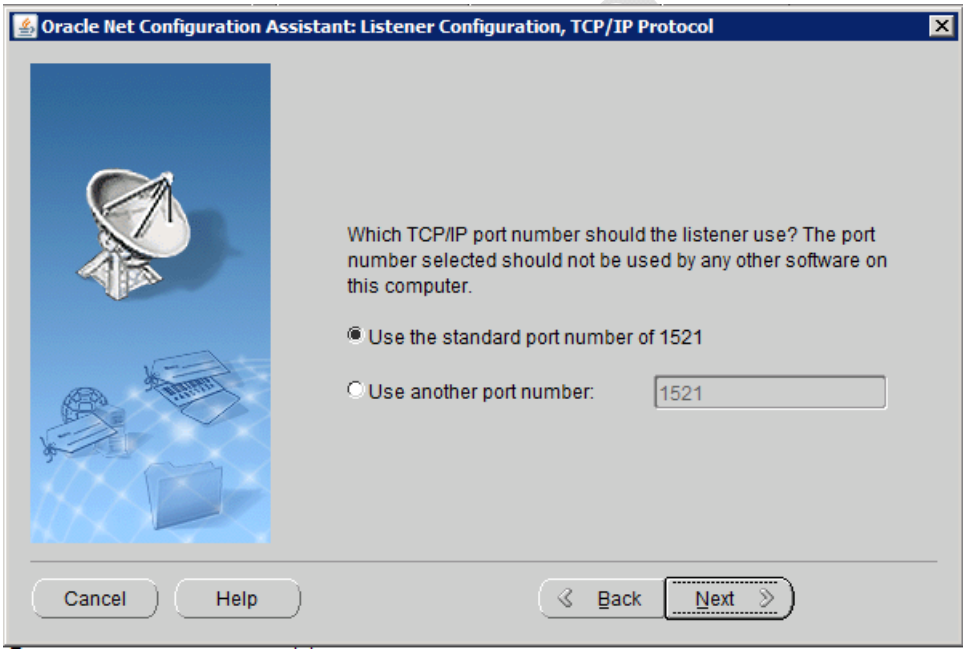


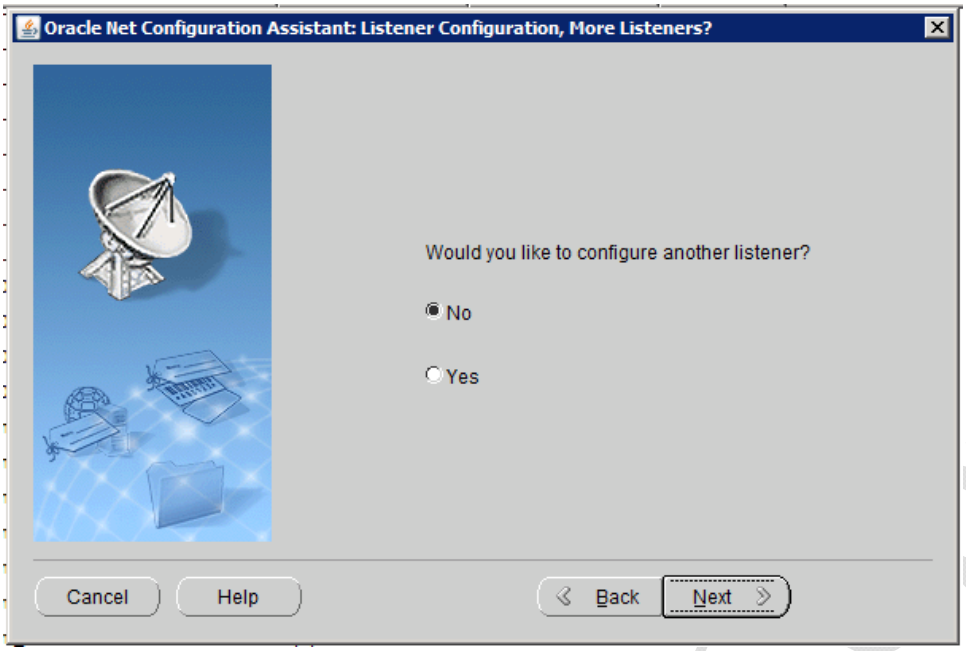
Oracle net configuration asst



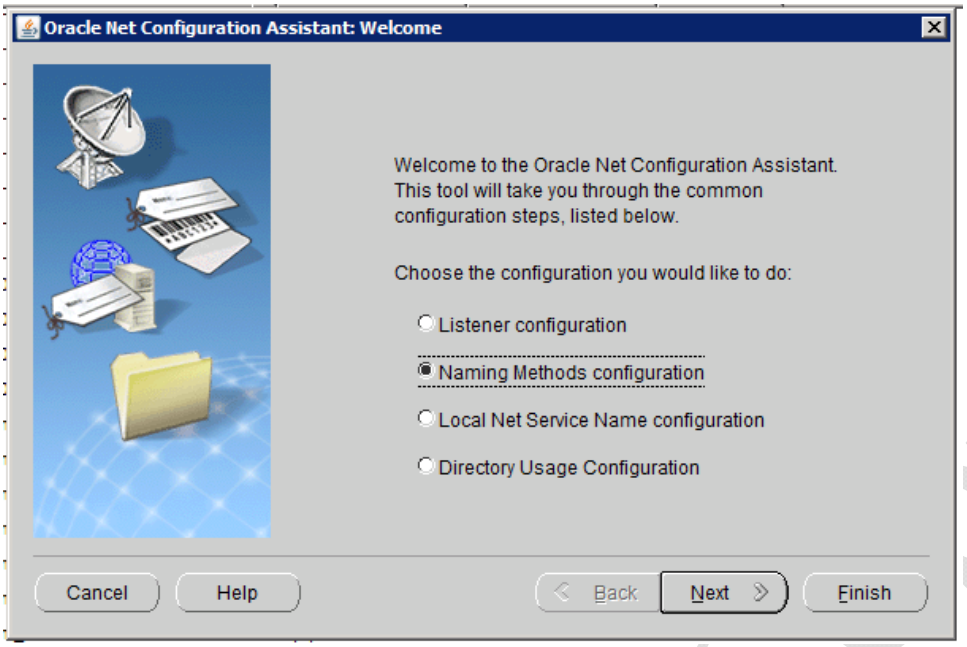


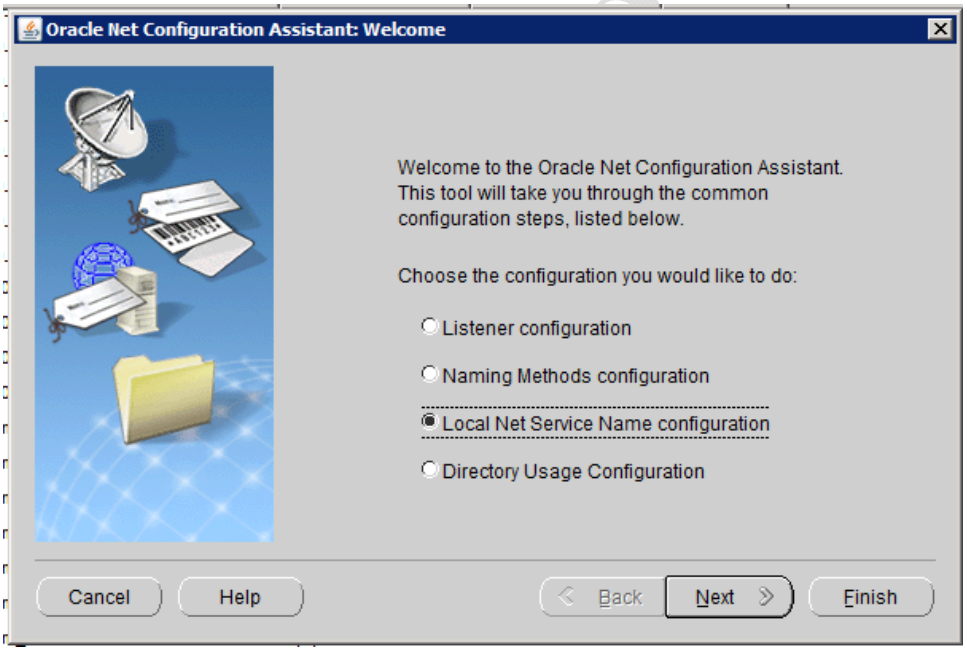

Oracle Net Configuration Assistant: Listener Configuration, Select Protocols
You can configure the listener to accept connections over one or more protocols. Select which protocols you want to configure for this listener. Keep your configuration as simple as possible by configuring only the protocols you need.
Available Protocols
TCPS
IPC
NMP
Selected Protocols
TCP
Cancel
Help
Back
Next

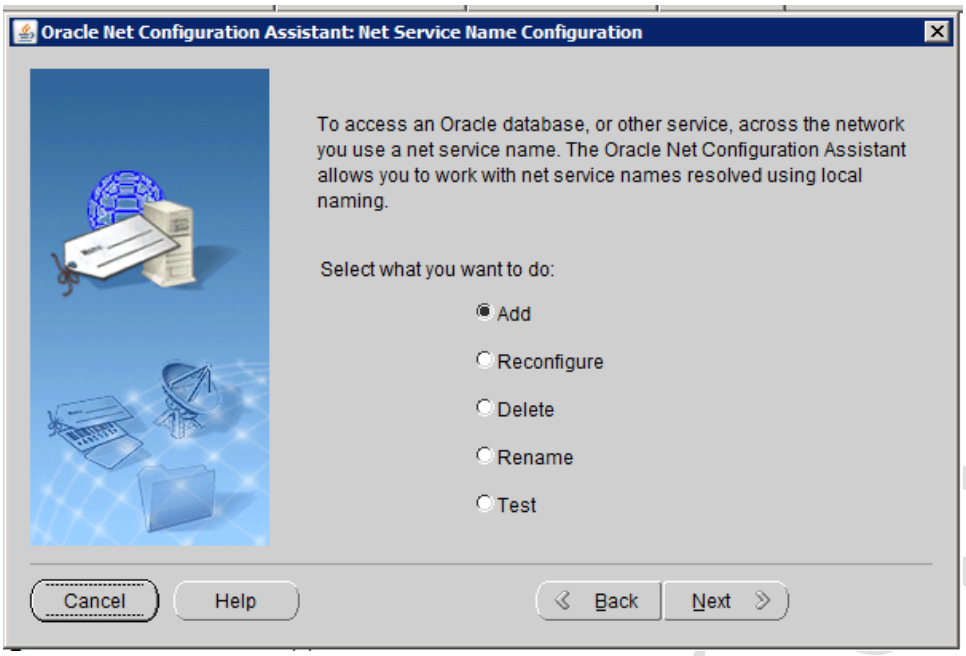

Oracle Net Configuration Assistant: Listener Configuration, TCP/IP Protocol
Which TCP/IP port number should the listener use? The port number selected should not be used by any other software on this computer.
Use the standard port number of 1521
Use another port number:
1521
Cancel
Help
Back
Next

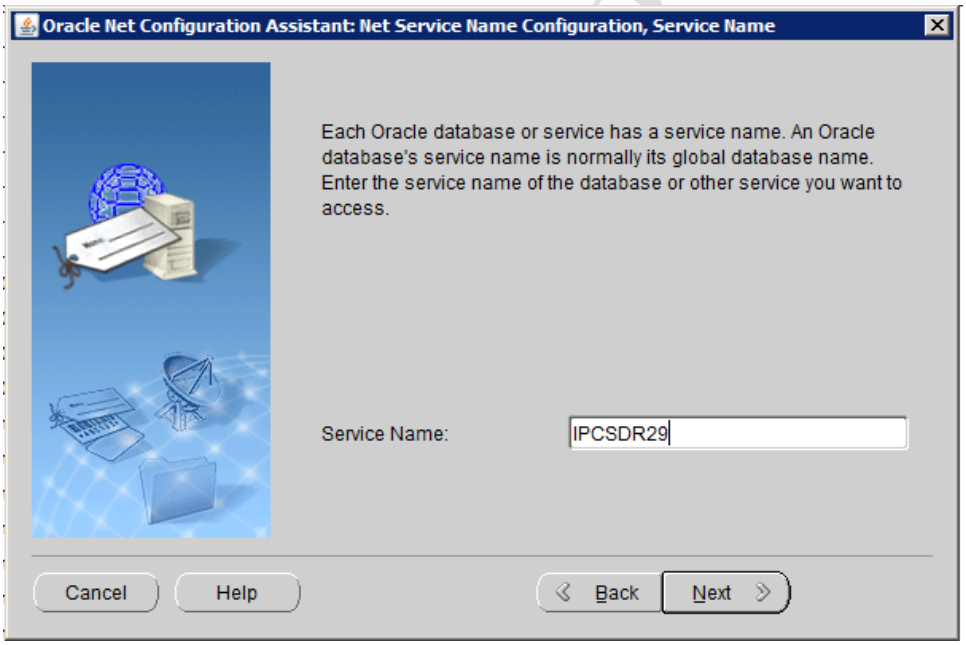

Oracle Net Configuration Assistant: Listener Configuration, More Listeners?
Would you like to configure another listener?
No
Yes
Cancel
Help
Back
Next

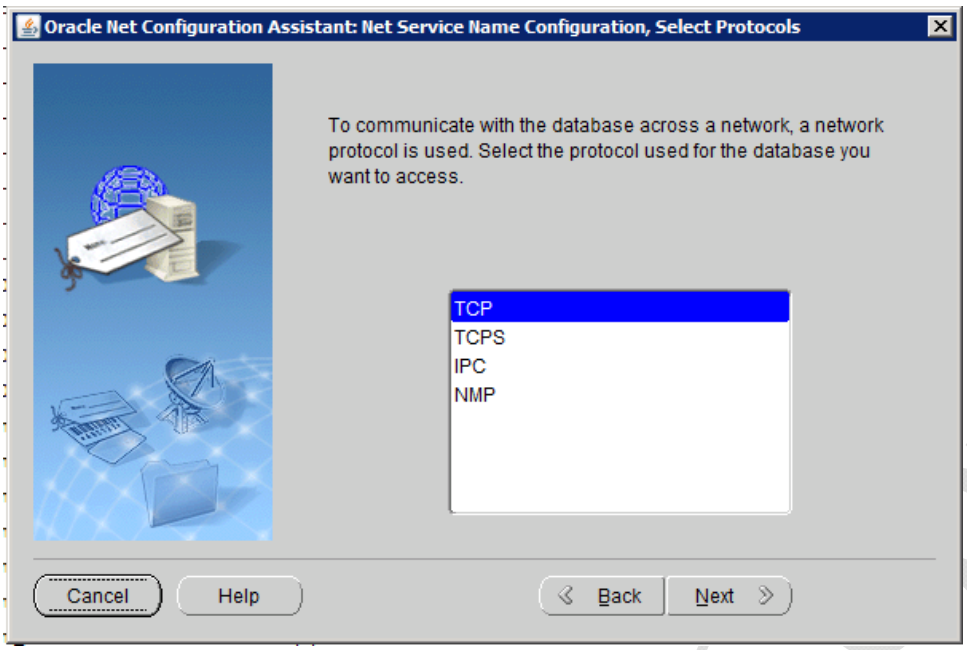

Oracle Net Configuration Assistant: Listener Configuration Done
Listener configuration complete!
Cancel
Help
Back
Next

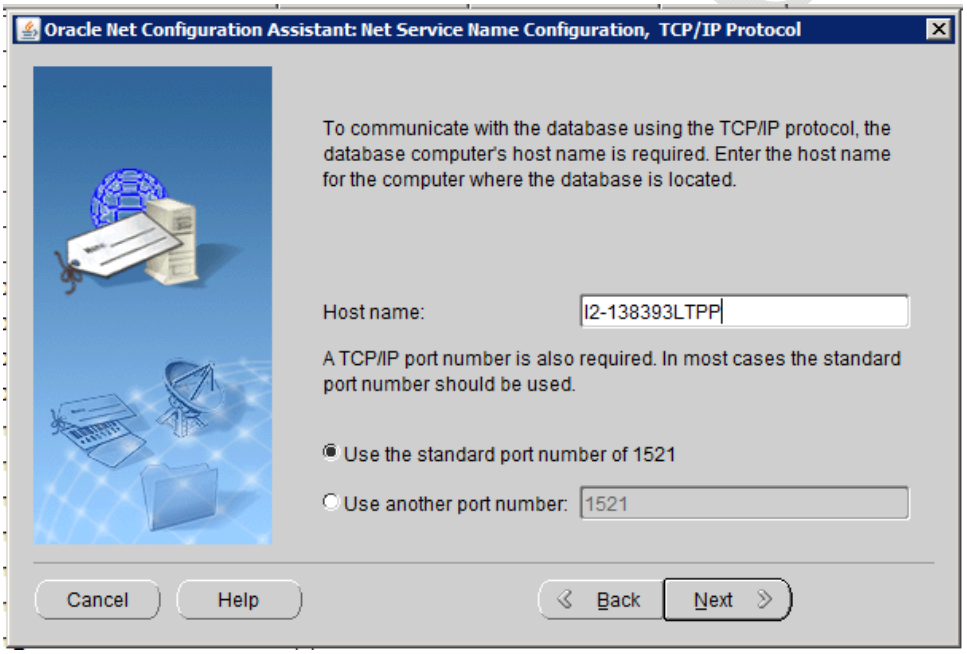

Oracle Net Configuration Assistant: Welcome
Welcome to the Oracle Net Configuration Assistant.
This tool will take you through the common
configuration steps, listed below.
Choose the configuration you would like to do:
Listener configuration
Naming Methods configuration
Local Net Service Name configuration
Directory Usage Configuration
Cancel
Help
Back
Next
Finish

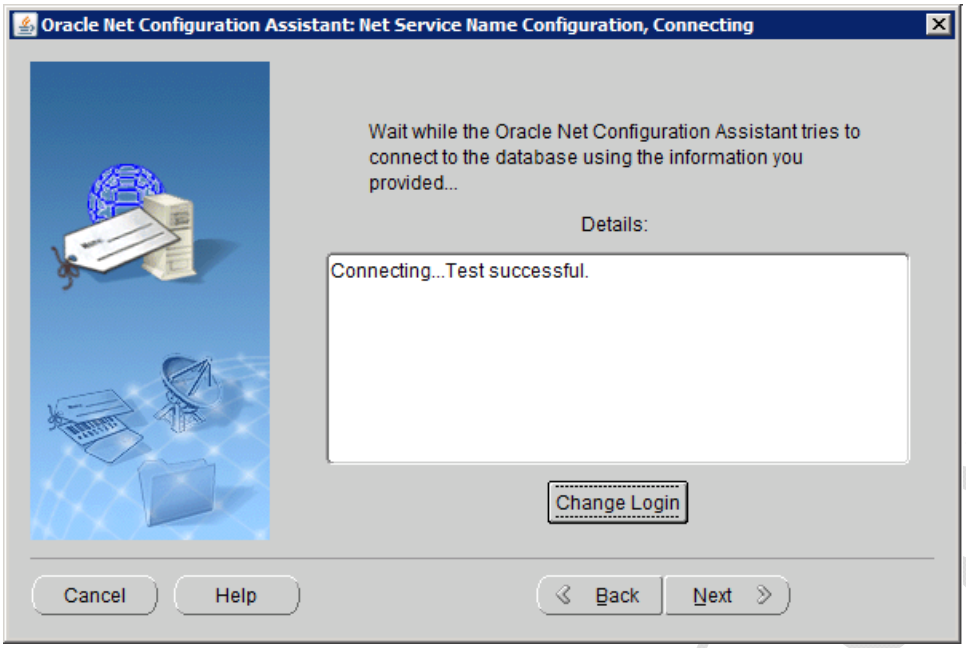

Oracle Net Configuration Assistant: Welcome
Welcome to the Oracle Net Configuration Assistant.
This tool will take you through the common
configuration steps, listed below.
Choose the configuration you would like to do:
Listener configuration
Naming Methods configuration
Local Net Service Name configuration
Directory Usage Configuration
Cancel
Help
Back
Next
Finish

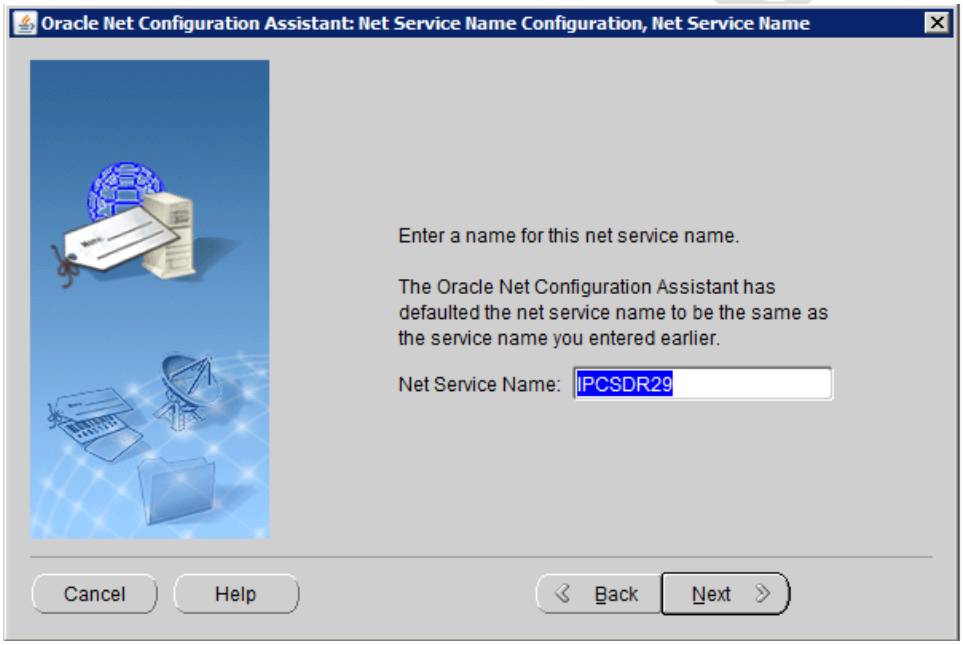

Oracle Net Configuration Assistant: Net Service Name Configuration
To access an Oracle database, or other service, across the network you use a net service name. The Oracle Net Configuration Assistant allows you to work with net service names resolved using local naming.
Select what you want to do:
Add
Reconfigure
Delete
Rename
Test
Cancel
Help
Back
Next

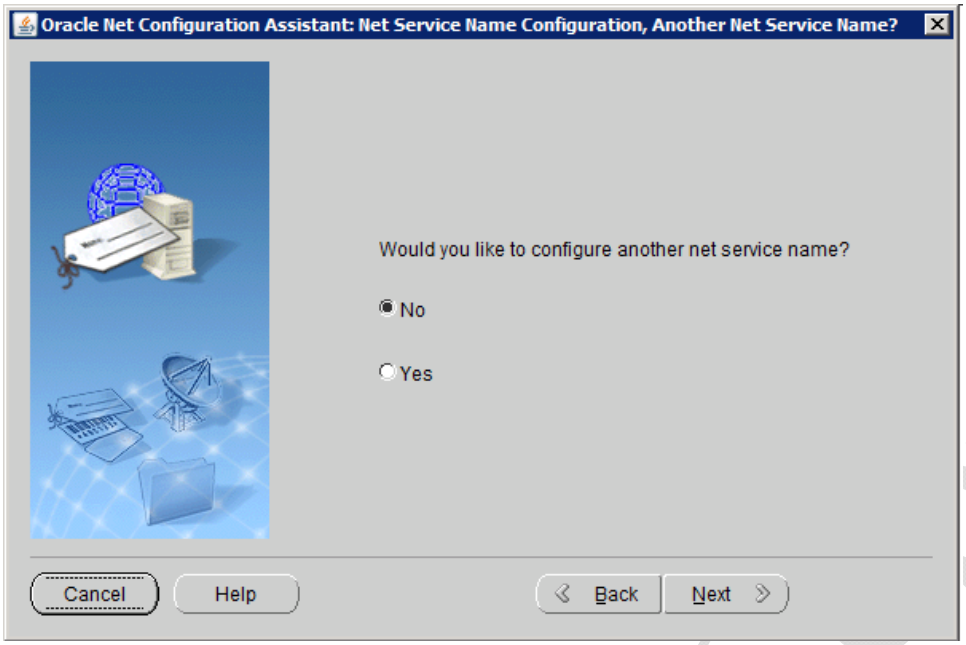

Oracle Net Configuration Assistant: Net Service Name Configuration, Service Name
Each Oracle database or service has a service name. An Oracle database's service name is normally its global database name. Enter the service name of the database or other service you want to access.
Service Name:
IPCSDR29
Cancel
Help
Back
Next


Oracle Net Configuration Assistant: Net Service Name Configuration, Select Protocols
To communicate with the database across a network, a network protocol is used. Select the protocol used for the database you want to access.
TCP
TCPS
IPC
NMP
Cancel
Help
Back
Next

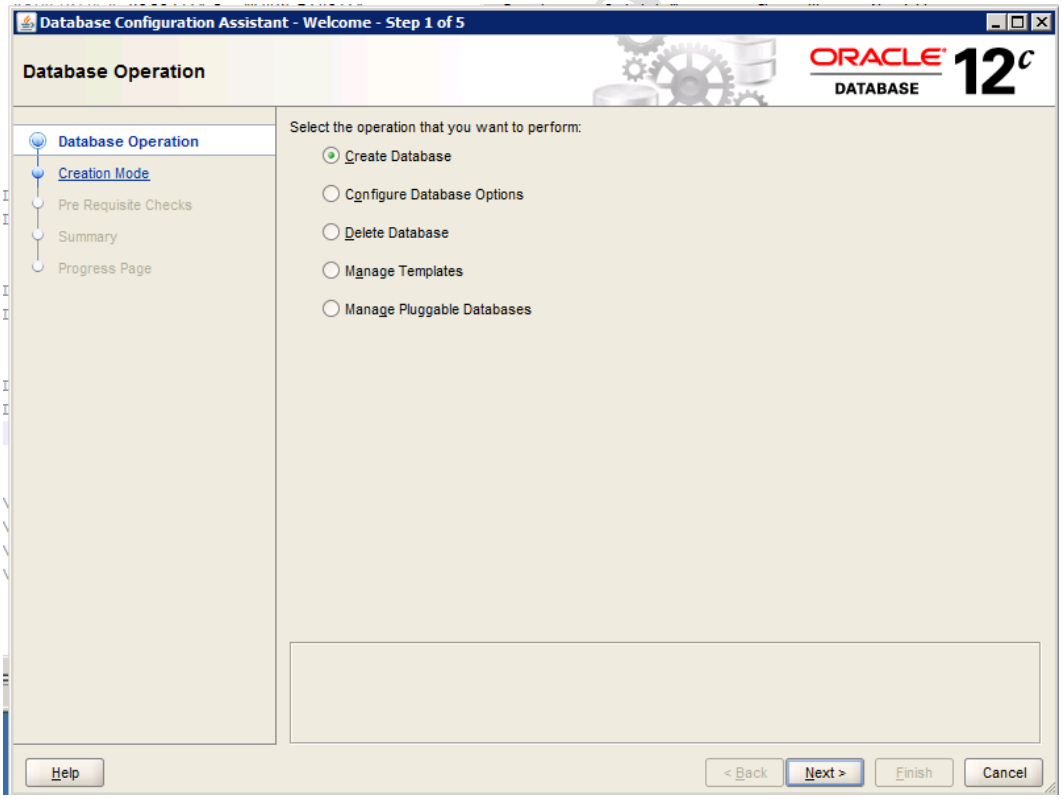

Oracle Net Configuration Assistant: Net Service Name Configuration, TCP/IP Protocol
To communicate with the database using the TCP/IP protocol, the database computer's host name is required. Enter the host name for the computer where the database is located.
Host name:
I2-138393LTPP
A TCP/IP port number is also required. In most cases the standard port number should be used.
Use the standard port number of 1521
Use another port number:
1521
Cancel
Help
Back
Next

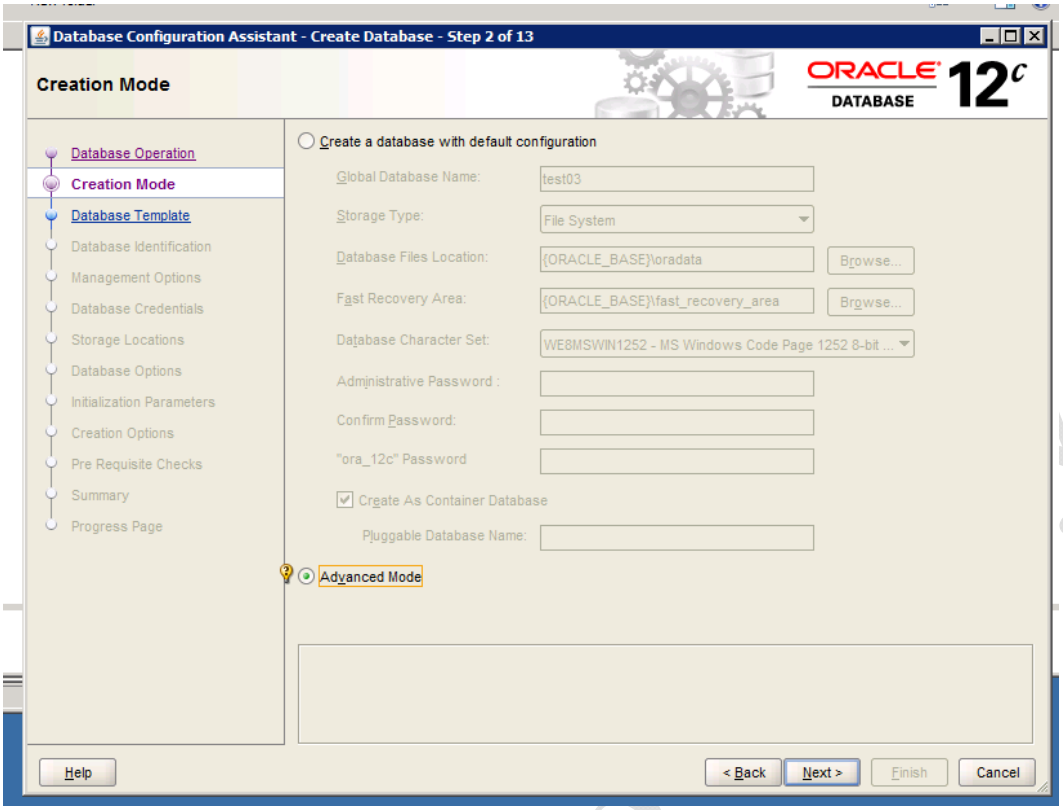

Oracle Net Configuration Assistant: Net Service Name Configuration, Connecting
Wait while the Oracle Net Configuration Assistant tries to connect to the database using the information you provided...
Details:
Connecting...Test successful.
Change Login
Cancel
Help
Back
Next

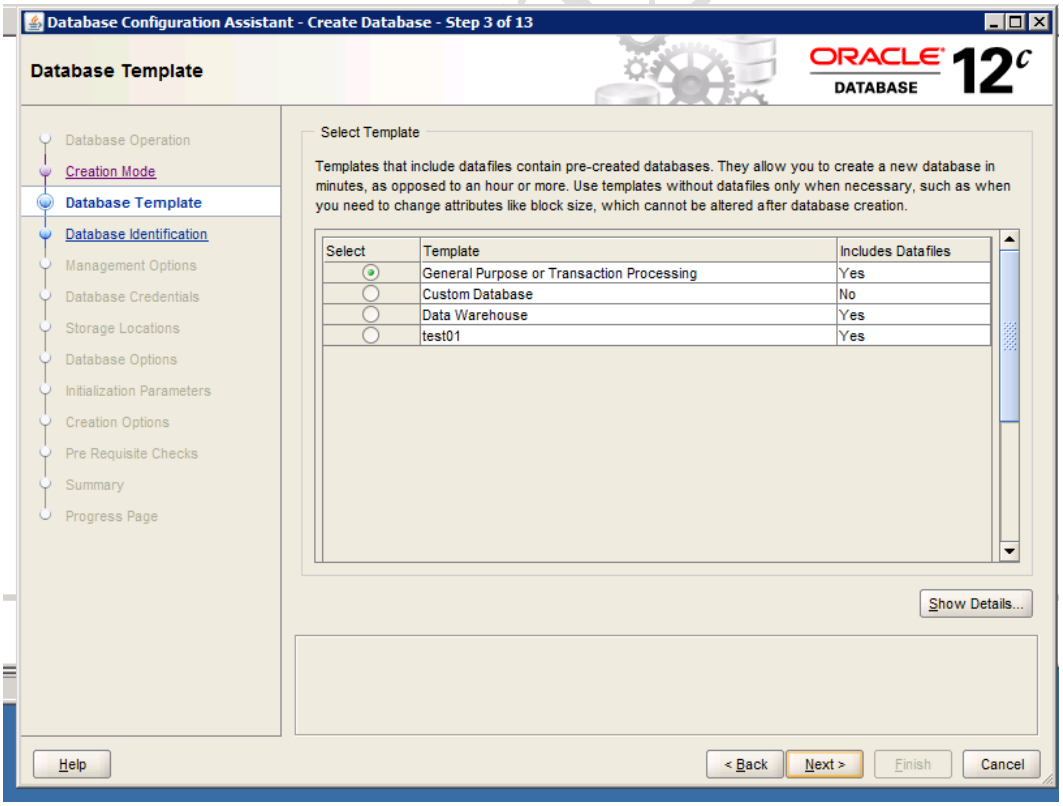

Oracle Net Configuration Assistant: Net Service Name Configuration, Net Service Name
Enter a name for this net service name.
The Oracle Net Configuration Assistant has defaulted the net service name to be the same as the service name you entered earlier.
Net Service Name:
IPCSDR29
Cancel
Help
Back
Next

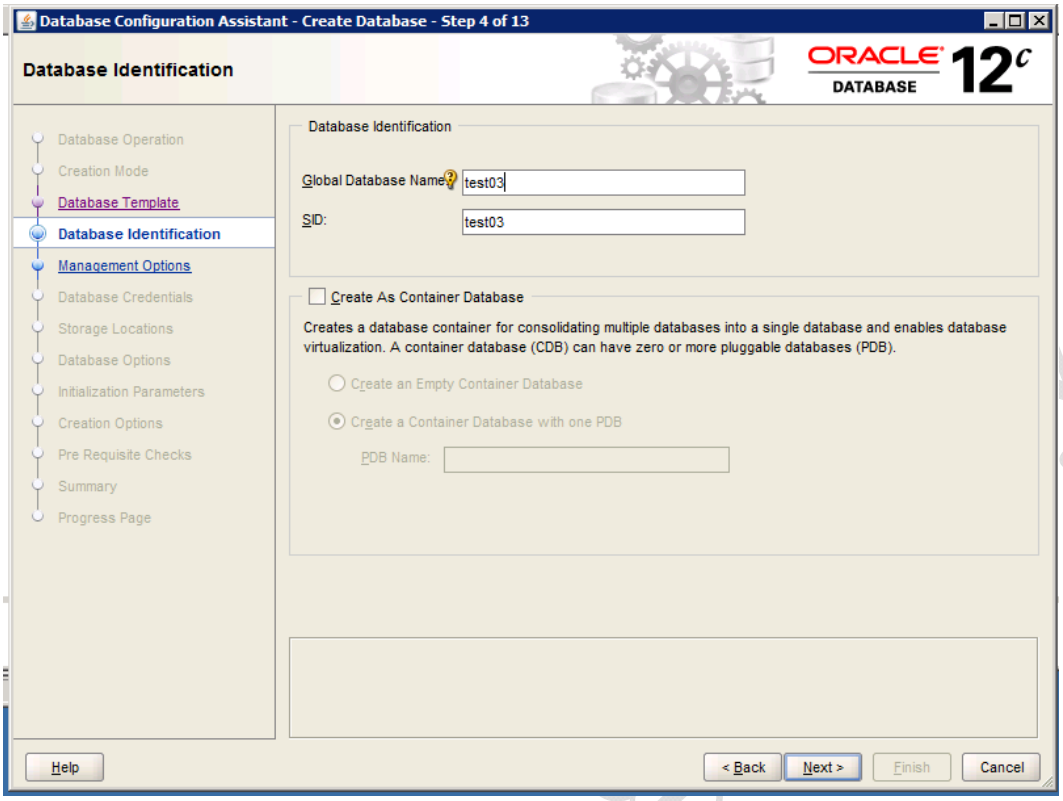


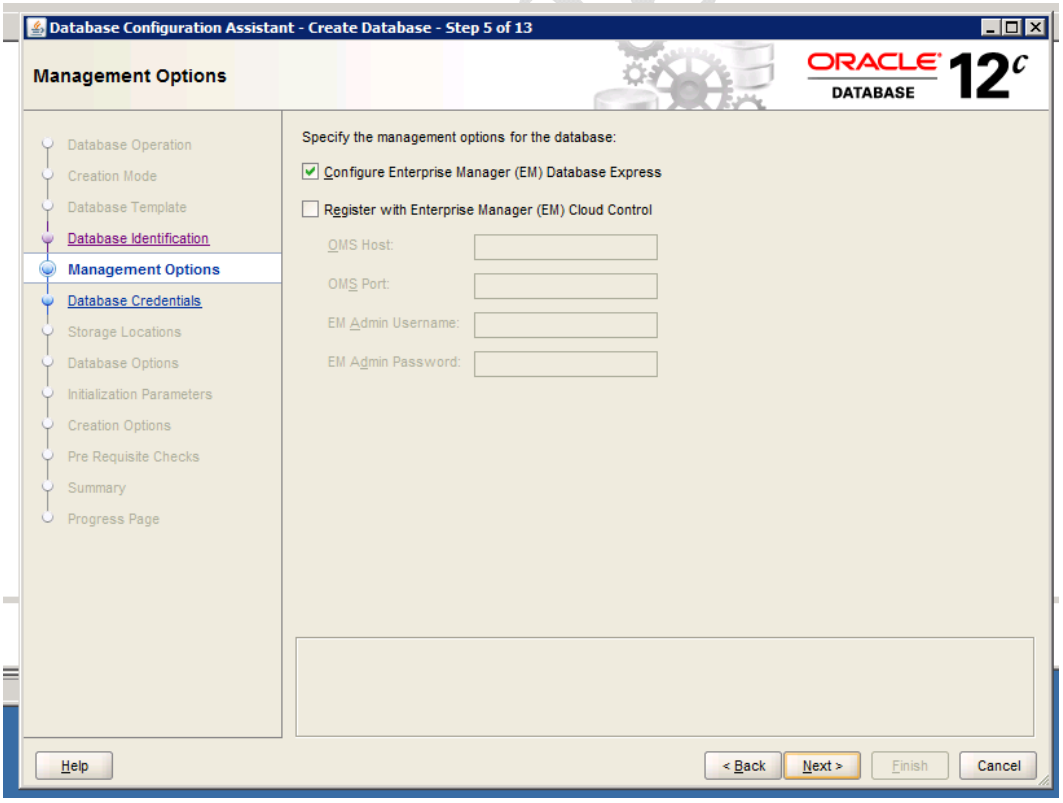
CREATING AN INSTANCE

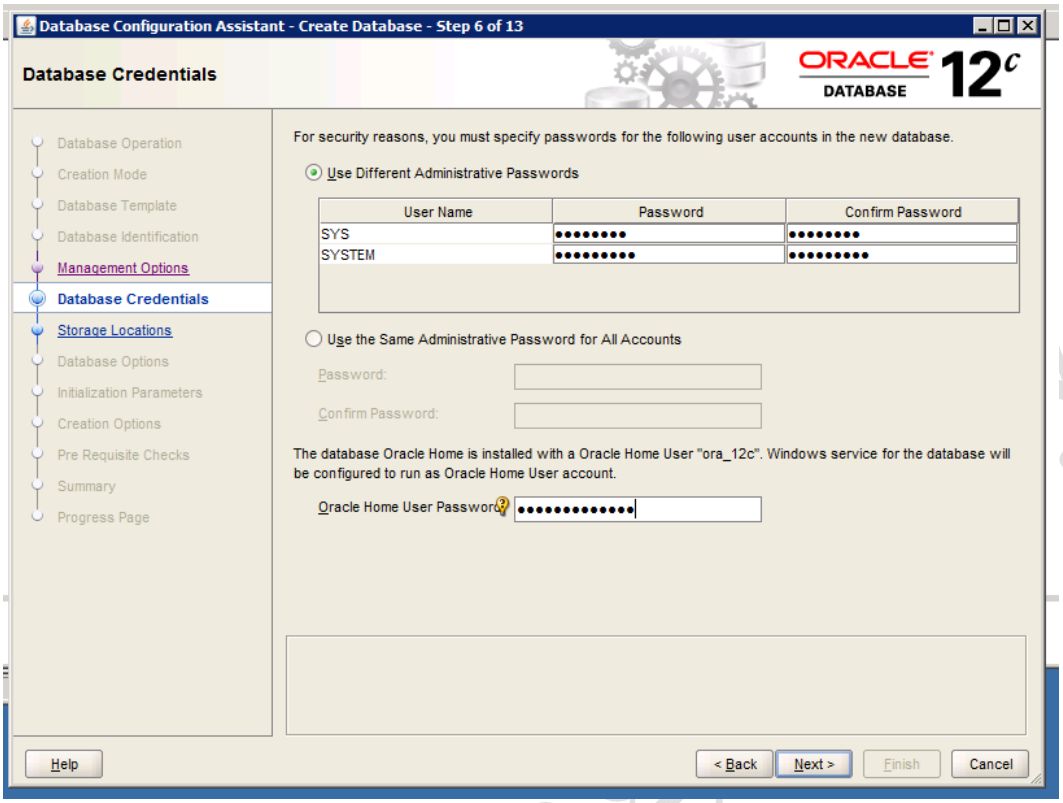


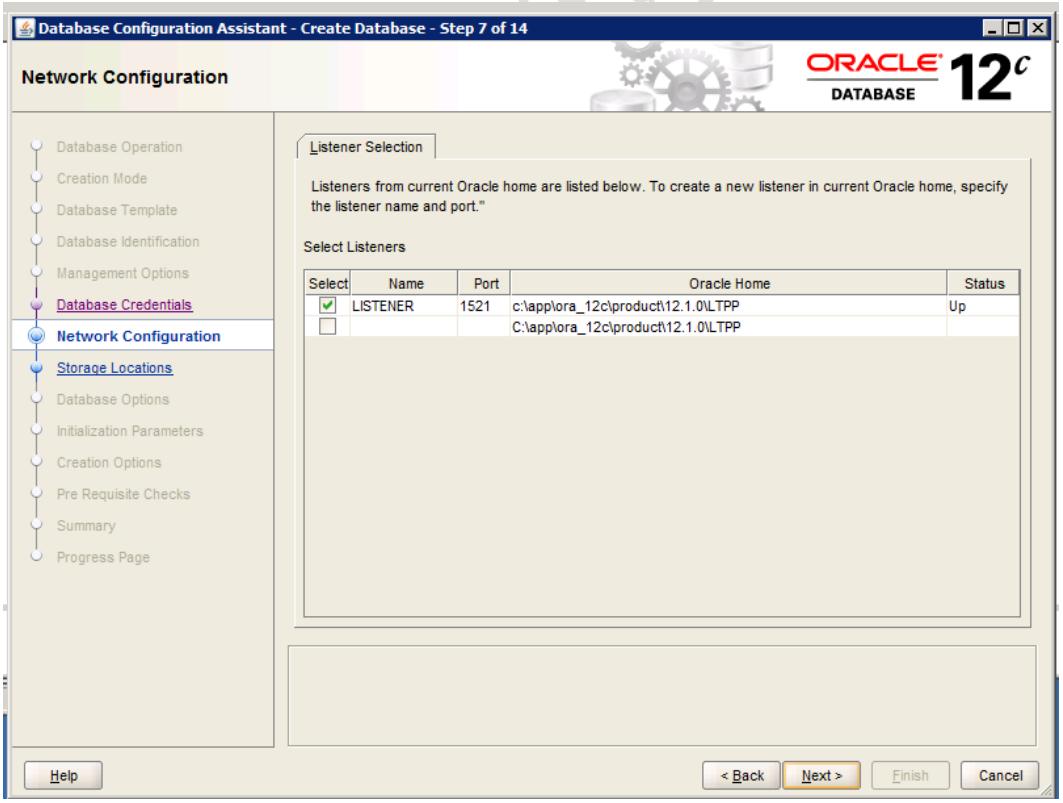

Database Configuration Assistant - Create Database - Step 2 of 13
Creation Mode
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Create a database with default configuration
Global Database Name: test03
Storage Type: File System
Database Files Location: {ORACLE_BASE}\oradata
Browse...
Fast Recovery Area: {ORACLE_BASE}\fast_recovery_area
Browse...
Database Character Set: WE8MSWIN1252 - MS Windows Code Page 1252 8-bit ...
Administrative Password :
Confirm Password:
"ora_12c" Password
Create As Container Database
Pluggable Database Name:
Advanced Mode
Help
< Back
Next >
Finish
Cancel

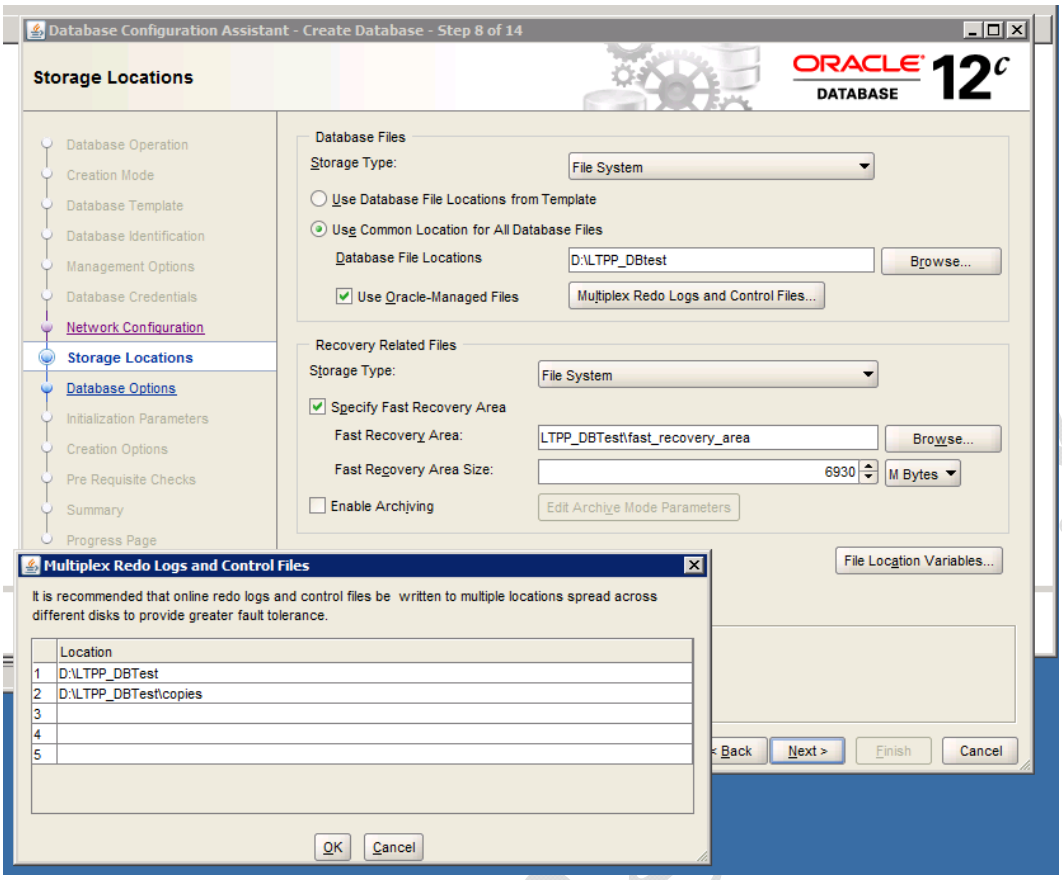

Database Configuration Assistant - Create Database - Step 3 of 13
Database Template
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Select Template
Templates that include datafiles contain pre-created databases. They allow you to create a new database in minutes, as opposed to an hour or more. Use templates without datafiles only when necessary, such as when you need to change attributes like block size, which cannot be altered after database creation.
Select
Template
Includes Datafiles
General Purpose or Transaction Processing
Yes
Custom Database
No
Data Warehouse
Yes
test01
Yes
Show Details...
Help
< Back
Next >
Finish
Cancel

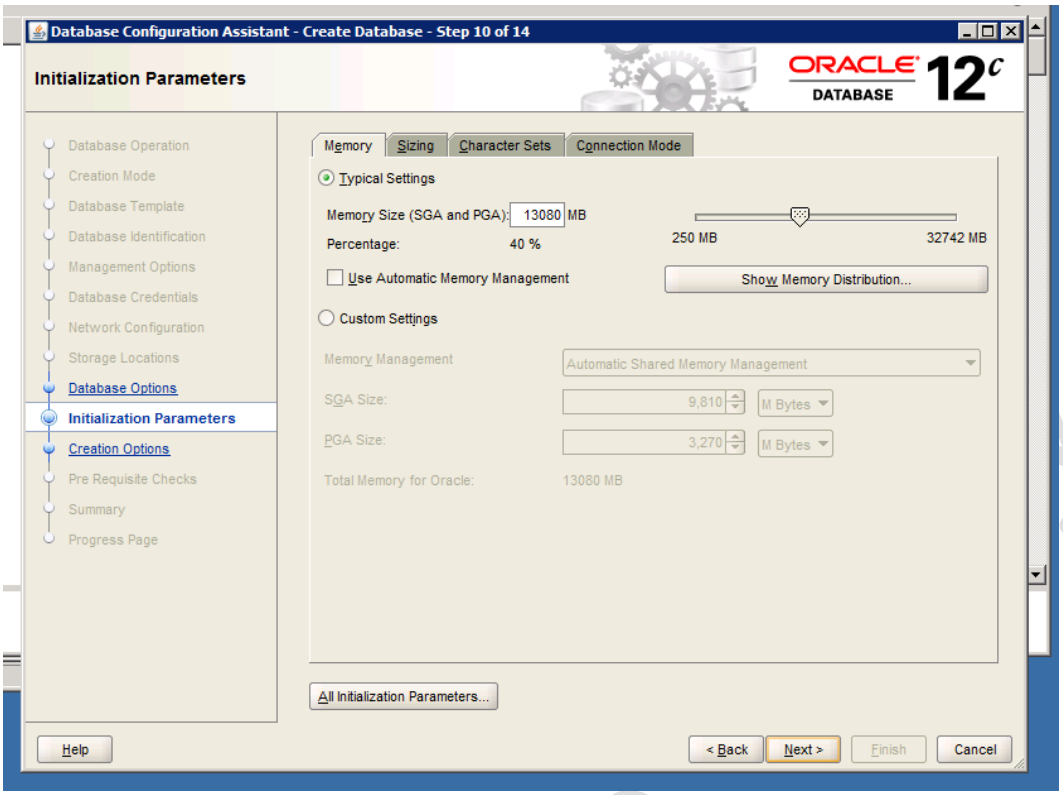

Database Configuration Assistant - Create Database - Step 4 of 13
Database Identification
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Database Identification
Global Database Name: test03
SID: test03
Create As Container Database
Creates a database container for consolidating multiple databases into a single database and enables database virtualization. A container database (CDB) can have zero or more pluggable databases (PDB).
Create an Empty Container Database
Create a Container Database with one PDB
PDB Name:
Help
< Back
Next >
Finish
Cancel

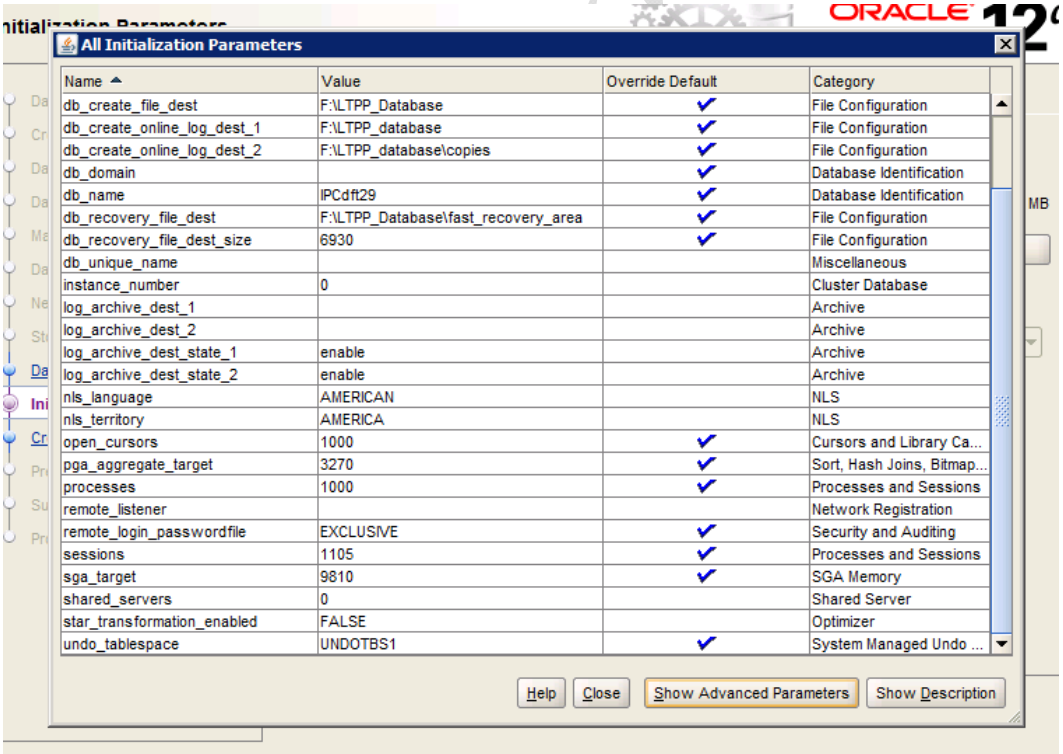

Database Configuration Assistant - Create Database - Step 5 of 13
Management Options
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Specify the management options for the database:
Configure Enterprise Manager (EM) Database Express
Register with Enterprise Manager (EM) Cloud Control
OMS Host:
OMS Port:
EM Admin Username:
EM Admin Password:
Help
< Back
Next >
Finish
Cancel

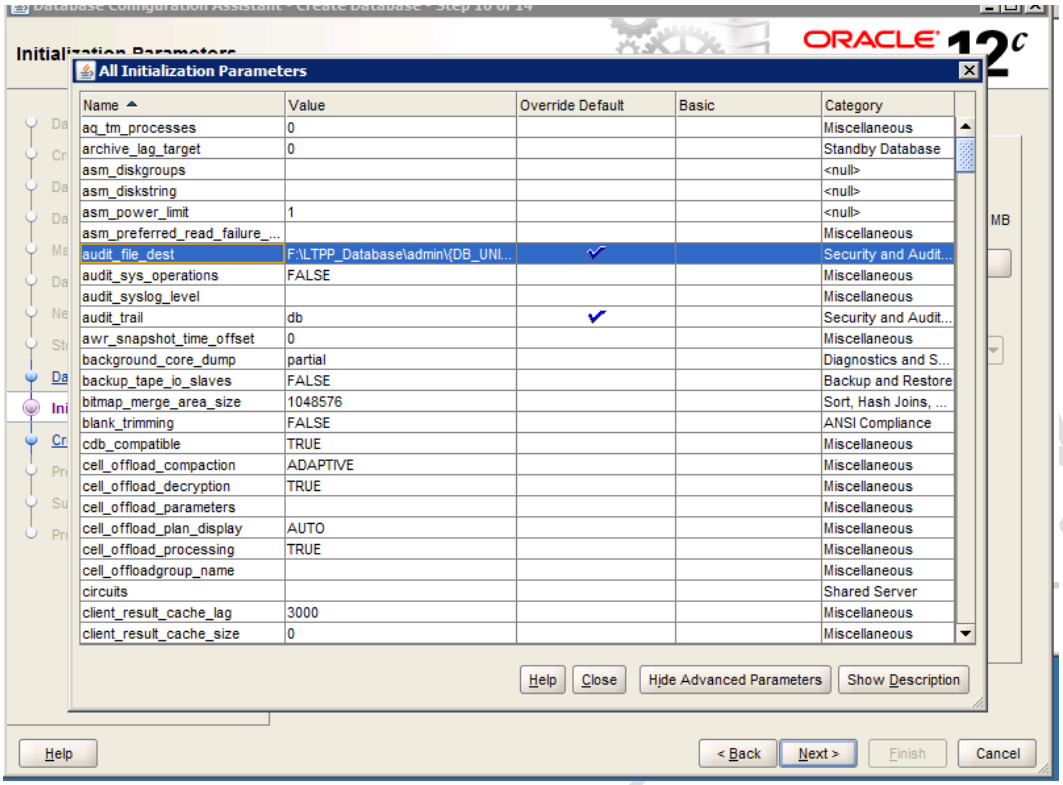

Database Configuration Assistant - Create Database - Step 6 of 13
Database Credentials
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
For security reasons, you must specify passwords for the following user accounts in the new database.
Use Different Administrative Passwords
User Name
Password
Confirm Password
SYS
SYSTEM
Use the Same Administrative Password for All Accounts
Password:
Confirm Password:
The database Oracle Home is installed with a Oracle Home User "ora_12c". Windows service for the database will be configured to run as Oracle Home User account.
Oracle Home User Password:
Help
< Back
Next >
Finish
Cancel

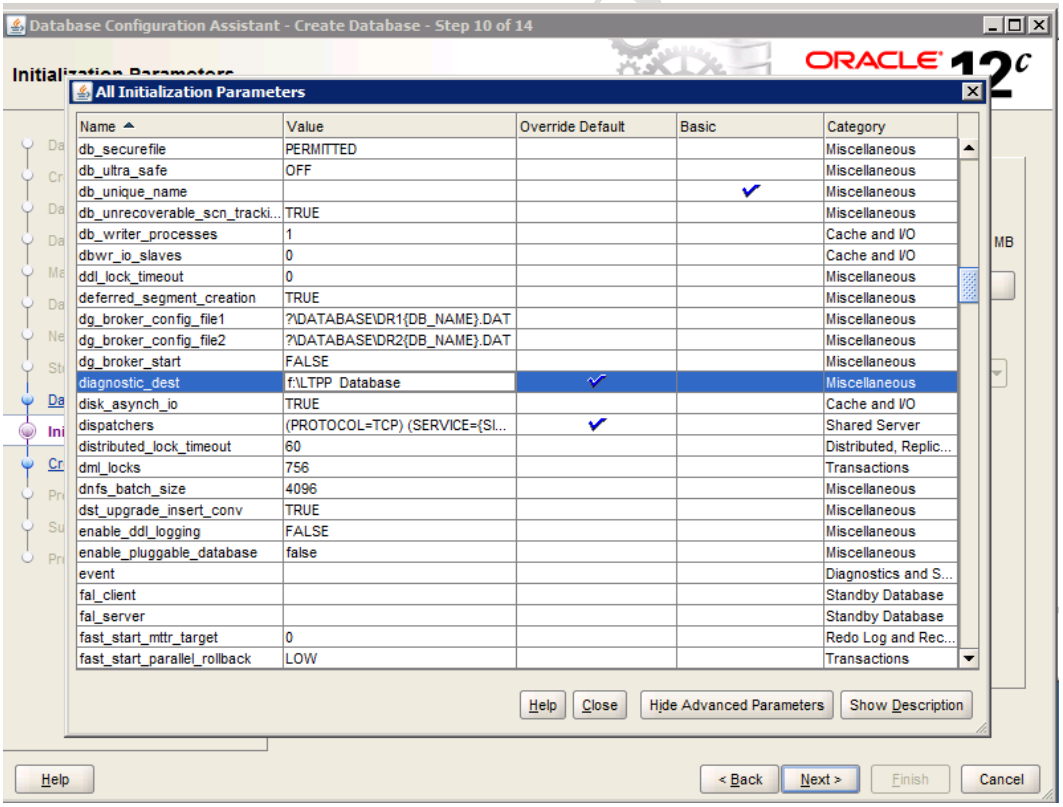

Database Configuration Assistant - Create Database - Step 7 of 14
Network Configuration
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Network Configuration
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Listener Selection
Listeners from current Oracle home are listed below. To create a new listener in current Oracle home, specify the listener name and port."
Select Listeners
Select
Name
Port
Oracle Home
Status
LISTENER
1521
c:\app\ora_12c\product\12.1.0\LTPP
Up
C:\app\ora_12c\product\12.1.0\LTPP
Help
< Back
Next >
Finish
Cancel

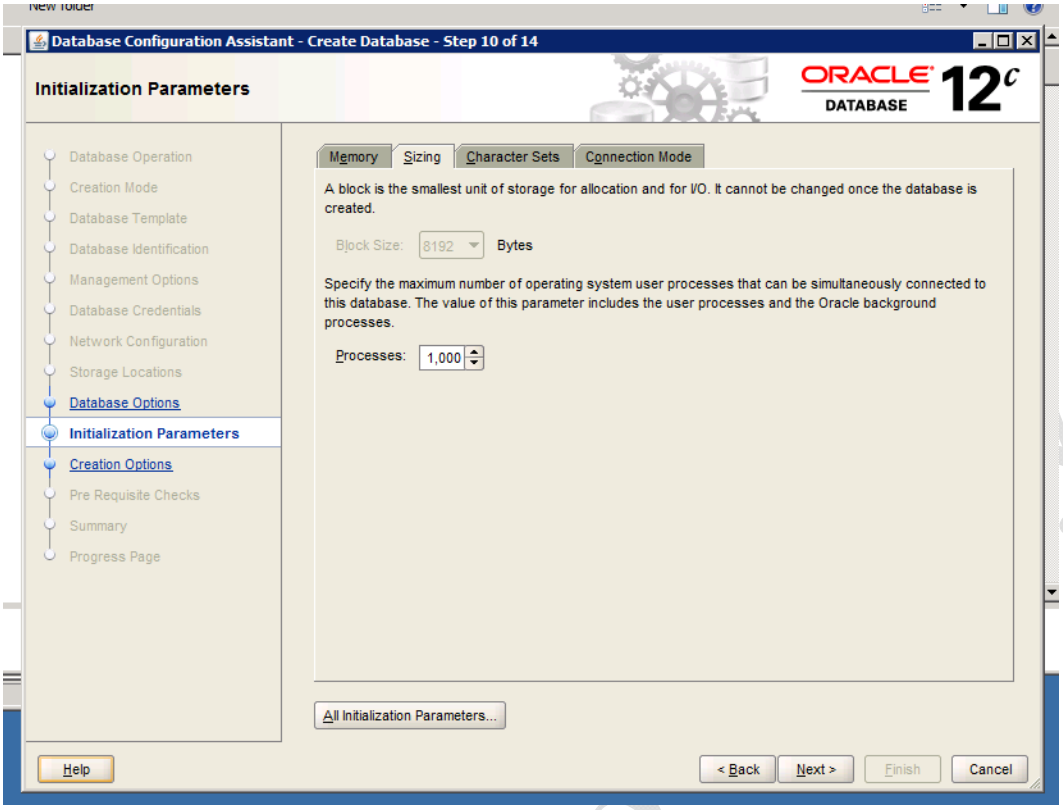

Database Configuration Assistant - Create Database - Step 8 of 14
Storage Locations
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Network Configuration
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Database Files
Storage Type:
File System
Use Database File Locations from Template
Use Common Location for All Database Files
Database File Locations
D:\LTPP_DBtest
Browse...
Use Oracle-Managed Files
Multiplex Redo Logs and Control Files...
Recovery Related Files
Storage Type:
File System
Specify Fast Recovery Area
Fast Recovery Area:
LTPP_DBTest\fast_recovery_area
Browse...
Fast Recovery Area Size:
6930
M Bytes
Enable Archiving
Edit Archive Mode Parameters
File Location Variables...
Back
Next >
Finish
Cancel
Multiplex Redo Logs and Control Files
It is recommended that online redo logs and control files be written to multiple locations spread across different disks to provide greater fault tolerance.
Location
1 D:\LTPP_DBTest
2 D:\LTPP_DBTest\copies
3
4
5
OK
Cancel

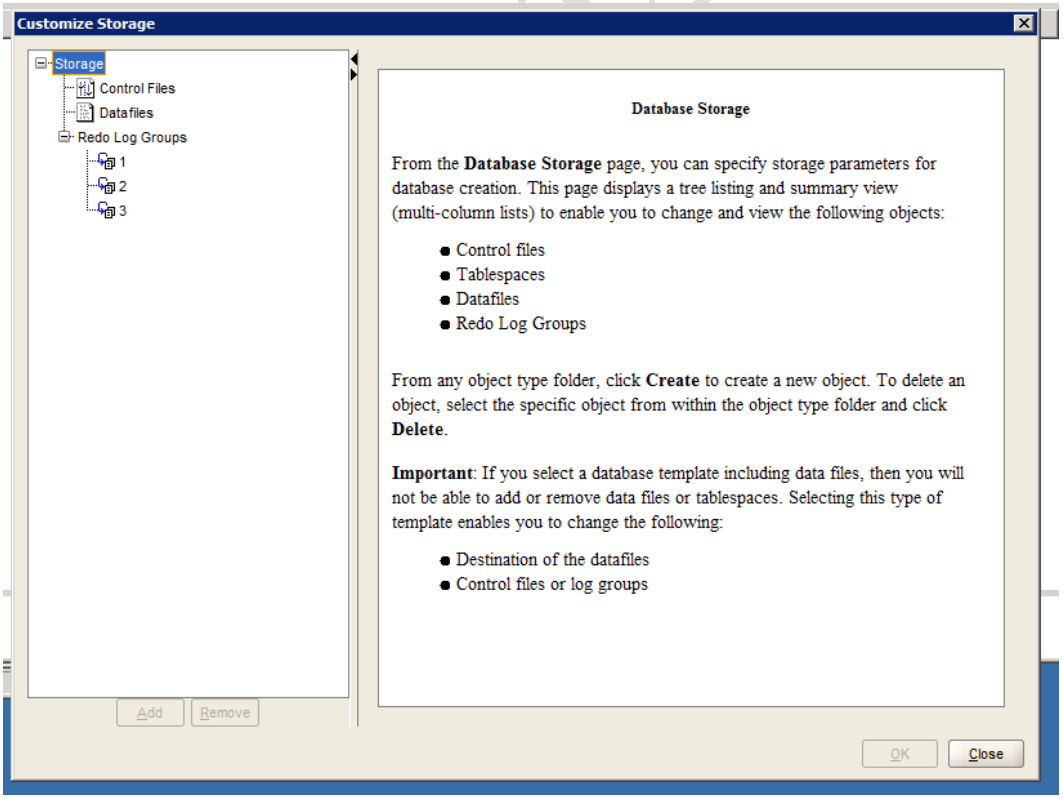

Database Configuration Assistant - Create Database - Step 10 of 14
Initialization Parameters
ORACLE DATABASE 12c
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Network Configuration
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Memory
Sizing
Character Sets
Connection Mode
Typical Settings
Memory Size (SGA and PGA): 13080 MB
Percentage: 40 %
250 MB
32742 MB
Use Automatic Memory Management
Show Memory Distribution...
Custom Settings
Memory Management
Automatic Shared Memory Management
SGA Size:
9,810
M Bytes
PGA Size:
3,270
M Bytes
Total Memory for Oracle:
13080 MB
All Initialization Parameters...
Help
< Back
Next >
Finish
Cancel

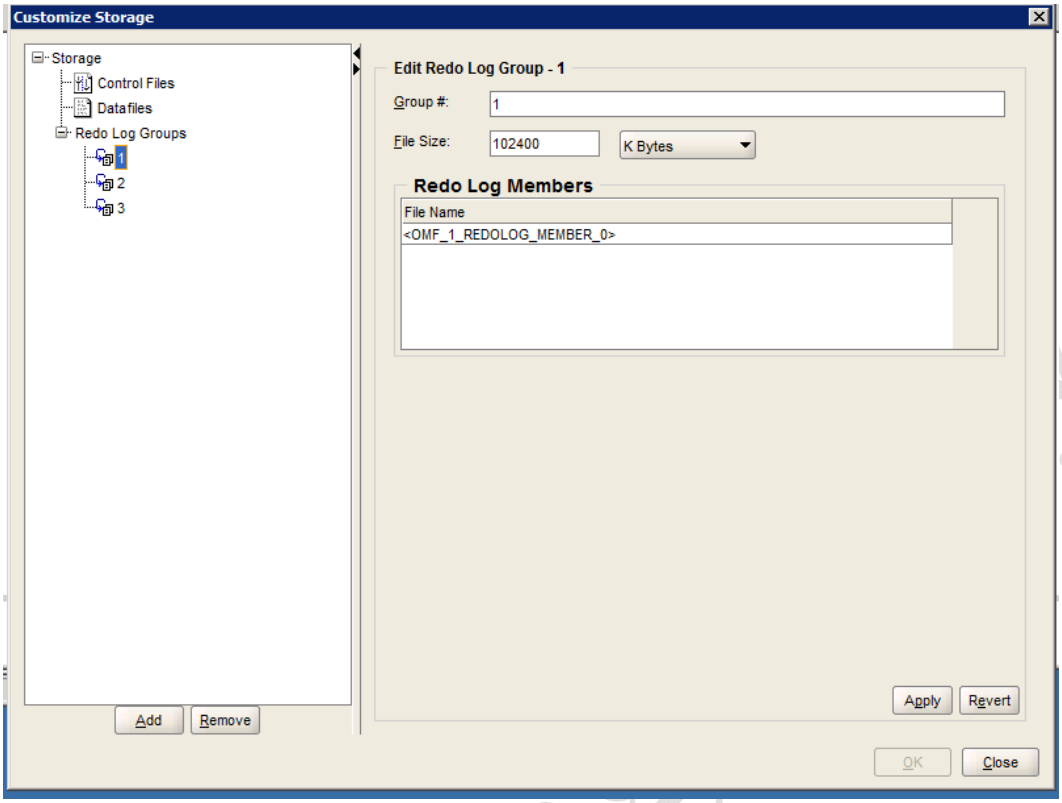

All Initialization Parameters
Name
Value
Override Default
Category
db_create_file_dest
F:\LTPP_Database
File Configuration
db_create_online_log_dest_1
F:\LTPP_database
File Configuration
db_create_online_log_dest_2
F:\LTPP_database\copies
File Configuration
db_domain
Database Identification
db_name
IPCdft29
Database Identification
db_recovery_file_dest
F:\LTPP_Database\fast_recovery_area
File Configuration
db_recovery_file_dest_size
6930
File Configuration
db_unique_name
Miscellaneous
instance_number
0
Cluster Database
log_archive_dest_1
Archive
log_archive_dest_2
Archive
log_archive_dest_state_1
enable
Archive
log_archive_dest_state_2
enable
Archive
nls_language
AMERICAN
NLS
nls_territory
AMERICA
NLS
open_cursors
1000
Cursors and Library Ca...
pga_aggregate_target
3270
Sort, Hash Joins, Bitmap...
processes
1000
Processes and Sessions
remote_listener
Network Registration
remote_login_passwordfile
EXCLUSIVE
Security and Auditing
sessions
1105
Processes and Sessions
sga_target
9810
SGA Memory
shared_servers
0
Shared Server
star_transformation_enabled
FALSE
Optimizer
undo_tablespace
UNDOTBS1
System Managed Undo ...
Help
Close
Show Advanced Parameters
Show Description


All Initialization Parameters
Name
Value
Override Default
Basic
Category
aq_tm_processes 0 Miscellaneous
archive_lag_target 0 Standby Database
asm_diskgroups <null>
asm_diskstring <null>
asm_power_limit 1 <null>
asm_preferred_read_failure_... Miscellaneous
audit_file_dest F:\LTPP_Database\admin\{DB_UNI... Security and Audit...
audit_sys_operations FALSE Miscellaneous
audit_syslog_level Miscellaneous
audit_trail db Security and Audit...
awr_snapshot_time_offset 0 Miscellaneous
background_core_dump partial Diagnostics and S...
backup_tape_io_slaves FALSE Backup and Restore
bitmap_merge_area_size 1048576 Sort, Hash Joins, ...
blank_trimming FALSE ANSI Compliance
cdb_compatible TRUE Miscellaneous
cell_offload_compaction ADAPTIVE Miscellaneous
cell_offload_decryption TRUE Miscellaneous
cell_offload_parameters Miscellaneous
cell_offload_plan_display AUTO Miscellaneous
cell_offload_processing TRUE Miscellaneous
cell_offloadgroup_name Miscellaneous
circuits Shared Server
client_result_cache_lag 3000 Miscellaneous
client_result_cache_size 0 Miscellaneous
Help
Close
Hide Advanced Parameters
Show Description
Help
< Back
Next >
Finish
Cancel


Database Configuration Assistant - Create Database - Step 10 of 14
All Initialization Parameters
Name
Value
Override Default
Basic
Category
db_securefile PERMITTED Miscellaneous
db_ultra_safe OFF Miscellaneous
db_unique_name Miscellaneous
db_unrecoverable_scn_tracki... TRUE Miscellaneous
db_writer_processes 1 Cache and I/O
dbwr_io_slaves 0 Cache and I/O
ddl_lock_timeout 0 Miscellaneous
deferred_segment_creation TRUE Miscellaneous
dg_broker_config_file1 ?\DATABASE\DR1{DB_NAME}.DAT Miscellaneous
dg_broker_config_file2 ?\DATABASE\DR2{DB_NAME}.DAT Miscellaneous
dg_broker_start FALSE Miscellaneous
diagnostic_dest f:\LTPP_Database Miscellaneous
disk_asynch_io TRUE Cache and I/O
dispatchers (PROTOCOL=TCP) (SERVICE={SI... Shared Server
distributed_lock_timeout 60 Distributed, Replic...
dml_locks 756 Transactions
dnfs_batch_size 4096 Miscellaneous
dst_upgrade_insert_conv TRUE Miscellaneous
enable_ddl_logging FALSE Miscellaneous
enable_pluggable_database false Miscellaneous
event Diagnostics and S...
fal_client Standby Database
fal_server Standby Database
fast_start_mttr_target 0 Redo Log and Rec...
fast_start_parallel_rollback LOW Transactions
Help
Close
Hide Advanced Parameters
Show Description
Help
< Back
Next >
Finish
Cancel


Database Configuration Assistant - Create Database - Step 10 of 14
Initialization Parameters
ORACLE 12c DATABASE
Database Operation
Creation Mode
Database Template
Database Identification
Management Options
Database Credentials
Network Configuration
Storage Locations
Database Options
Initialization Parameters
Creation Options
Pre Requisite Checks
Summary
Progress Page
Memory
Sizing
Character Sets
Connection Mode
A block is the smallest unit of storage for allocation and for I/O. It cannot be changed once the database is created.
Block Size: 8192 Bytes
Specify the maximum number of operating system user processes that can be simultaneously connected to this database. The value of this parameter includes the user processes and the Oracle background processes.
Processes: 1,000
All Initialization Parameters...
Help
< Back
Next >
Finish
Cancel


Customize Storage
Storage
Control Files
Datafiles
Redo Log Groups
1
2
3
Add
Remove
Database Storage
From the Database Storage page, you can specify storage parameters for database creation. This page displays a tree listing and summary view (multi-column lists) to enable you to change and view the following objects:
Control files
Tablespaces
Datafiles
Redo Log Groups
From any object type folder, click Create to create a new object. To delete an object, select the specific object from within the object type folder and click Delete.
Important: If you select a database template including data files, then you will not be able to add or remove data files or tablespaces. Selecting this type of template enables you to change the following:
Destination of the datafiles
Control files or log groups
OK
Close


Customize Storage
Storage
Control Files
Datafiles
Redo Log Groups
1
2
3
Add
Remove
Edit Redo Log Group - 1
Group #:
1
File Size:
102400
K Bytes
Redo Log Members
File Name
<OMF_1_REDOLOG_MEMBER_0>
Apply
Revert
OK
Close

APPENDIX P. REMOTE ACCESS

Remote access to the central server from outside TFHRC is managed by FHWA IT at TFHRC over a VPN. Individuals holding DOT credentials are eligible to use the system. Individuals needing remote access must also have accounts on the LTPP servers.

The System Administrator and Backup System Administrator identified in Appendix A. Roles and Responsibilities – TFHRC Server, have remote access privileges. The TFHRC Help Desk also has remote access privileges through the internal TFHRC network to the servers.

Remote access is also used to work on the servers while at TFHRC. Due to noise concerns, limited time is actually spent in the server room. The TFHRC servers have multiple network cards. One card on each server is connected to a HP Procurve switch for use on an internal network. A non-COE machine located outside the server room is also connected to this internal network. The Dell 2900 is at 192. 168.2.25. The Dell R515 is at 192.168.2.26. The non-COE machine is at 192.168.2.37. Additional connections are available for LTPP FHWA staff but are not currently in use.

APPENDIX Q. ROLES AND RESPONSIBILITIES - DPW

The "Data Processing Workstation Disaster Recovery (DR) and Continuity of Operations Plan (COOP)" along with the "Data Processing Workstation IT Security Plan for the Long Term Pavement Performance Program" require that persons be identified to fulfill various roles. This section describes the roles required and the organizations providing individuals for those roles. The assignment of specific individuals by role and their contact information is provided quarterly to the COR who is the Information System Owner. This information is provided separately from this document to remove personally identifiable information (PII) and prevent obsolescence of this document.

The role assignments for this system are reviewed monthly. The organizations with individuals assigned to each role are documented in table 11. Contact information for each organization is provided in table 12.

- System Administrator – The system administrator is responsible for maintaining the DPW in good working order. This includes the operating system, access control, installed software, backups, and hardware.

- Backup System Administrator – The backup system administrator is responsible for maintaining the DPW under the direction of the system administrator and/or when the system administrator is unavailable. This includes the operating system, access control, installed software, backups, and hardware.

- DPW Database Administrator – The database administrator maintains the database instances on the DPW. This includes database backups, schema modification, and storage management.

- Backup DPW Database Administrator – The backup database administrator maintains the database instances on the DPW. This includes database backups, schema modification, and storage management under the direction of the database administrator and/or when the database administrator is unavailable.

- Regional Database Administrator – The regional database administrator oversees the maintenance of their regions data. They have the ability to modify their region's data using SQL scripts after TSSC review.

- Regional Program Manager – The regional program manager is responsible for the oversight of the data collection activities within the region.

- ADEP Power User – The ADEP power user is responsible for maintaining the files in the regional ADEP repository.

- PPDB Forms Edit – The PPDB forms edit role is responsible for data entry and maintenance using the PPDB forms.

- LTAS – The LTAS role allows the maintenance of traffic data using LTAS.

- SSH Users – The SSH users role allows users with a firewall account to use SSH to establish an encrypted tunnel to the database instances.

- Technical Support Services Contractor – The technical support services contractor role provides oversight for data collection and processing at the program level.

- Information System Owner – The information system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

- Authorizing Official – The authorizing is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

- Assignment of Security Responsibility –The assignment of security responsibility role is responsible for the overall security of the DPW.

- Other Designated Contacts – The other designated contacts role designates key contact personnel who can address inquiries regarding system characteristics and operation.

- FHWA - The FHWA role provides oversight to the LTPP program.

- Customer Service – The Customer Service role is responsible for answering customer inquiries including distributing data. Customer Service is also responsible for maintaining some centrally processed data.

Table 11. DPW Role assignments.

ROLE	Organization with Individuals in Role
System Administrator	AMEC
Backup System Administrator	AMEC
DPW Database Administrator	AMEC
Backup DPW Database Administrator	AMEC
Regional Database Administrator	Fugro NCE Stantec
Regional Program Manager	Fugro NCE Stantec

ROLE	Organization with Individuals in Role
ADEP Power User	AMEC ESCINC Fugro NCE SAIC Stantec
PPDB Forms Edit	AMEC ESCINC Fugro NCE SAIC Stantec
LTAS	AMEC Fugro NCE SAIC Stantec
SSH Users	AMEC Fugro NCE SAIC Stantec
Technical Support Services Contractor	AMEC SAIC
Information System Owner	FHWA
Customer Service	ESCINC
Authorizing Official	FHWA
Other Designated Contacts	SAIC
Assignment of Security Responsibility	SAIC
FHWA	See LTPP Team listing[2]

[2] http://www.fhwa.dot.gov/research/tfhrc/programs/infrastructure/pavements/ltpp/whoswho.cfm

Table 12. DPW - Organizational Contact Information.

Organization	Contact Information
Long Term Pavement Program Team (LTPP):	FHWA/DOT, HRDI-30 6300 Georgetown Pike McLean, VA 22101
SAIC:	151 Lafayette Drive Oak Ridge, TN 37830
AMEC Environment & Infrastructure (AMEC):	12000 Indian Creek Court, Suite F Beltsville, MD 20705 (301) 210-5105

Organization	Contact Information
Fugro Consultants, Inc (Fugro):	8613 Cross Park Drive Austin, Texas 78754 (512) 977-1800
NCE:	1885 S. Arlington Ave., Suite 111 Reno, NV 89509 (775) 329-4955
Stantec:	1000 Young Street, Suite #470 Tonawanda, NY 14150 (716) 632-0804
Engineering & Software Consultants, Inc. (ESCINC)	14123 Robert Paris Court Chantilly, VA 20151

APPENDIX R. CONTINUITY OF OPERATIONS – DPW

PURPOSE

The Continuity of Operations Plan (COOP) describes how the Long Term Pavement Performance (LTPP) Program will continue to function when the DPW is unable to sustain normal operations. The outage may be partial or total and may be the result of operator error, software problems, hardware problems, or network connectivity problems.

Scope

The scope of this COOP is the DPW.

Situation Overview

The DPW is used for the central archival of data gathered by the regional contractors. It provides the source of data disseminated to the public through standard media formats and on demand requests. Original copies of the data are maintained on the DPW and within the regions. Because the original data is not lost, it is possible for the THFRC server to be unavailable for a period of time without causing all data dissemination activity to stop. The primary risk to the system being unavailable is that delivery of data may be delayed beyond scheduled dates.

Planning Assumptions

The LTPP Team has agreed that three days of downtime would not have an adverse effect on data delivery. It has also been decided that if a hardware problem occurs with the server, the server will be repaired. Therefore there is not a failover system standing by. As explained later, we will rely on the Dell server maintenance and support agreement to repair the system in the event of a hardware failure.

Objectives

The objective of this plan is to outline the steps necessary to minimize disruption to LTPP data delivery in case of a system failure.

CONCEPT OF OPERATIONS

Phase I: Readiness and Preparedness

Knowing that system failures are inevitable, there are certain steps that can be taken ahead of time to ensure that services can be restored in a timely manner.

Backups

The server contains two Redundant Array of Independent Disks (RAID) volumes. The first volume is configured as a RAID 1 array consisting of two 1 TB Serial-Attached Small Computer System Interface (SAS) drives. This volume is the C: drive and contains

the operating system as well as a copy of the database backups, source code repository, and archive logs. This drive also hosts the bulk of the web applications. The RAID 1 array can withstand a single drive failure and remain operational. These drives are not hot swappable. The second volume is configured as a RAID 5 array consisting of seven 2 TB SAS drives. There is an eighth 2 TB SAS drive standing by as a hot spare. This array can withstand a single drive failure and the hot spare will automatically take the place of the failed drive providing additional protection until the failed drive can be replaced. These drives are hot swappable. This array is the D: drive and contains the database instances, ADEP repositories, and backup staging areas.

The diagram below shows the highlights of the backup process.

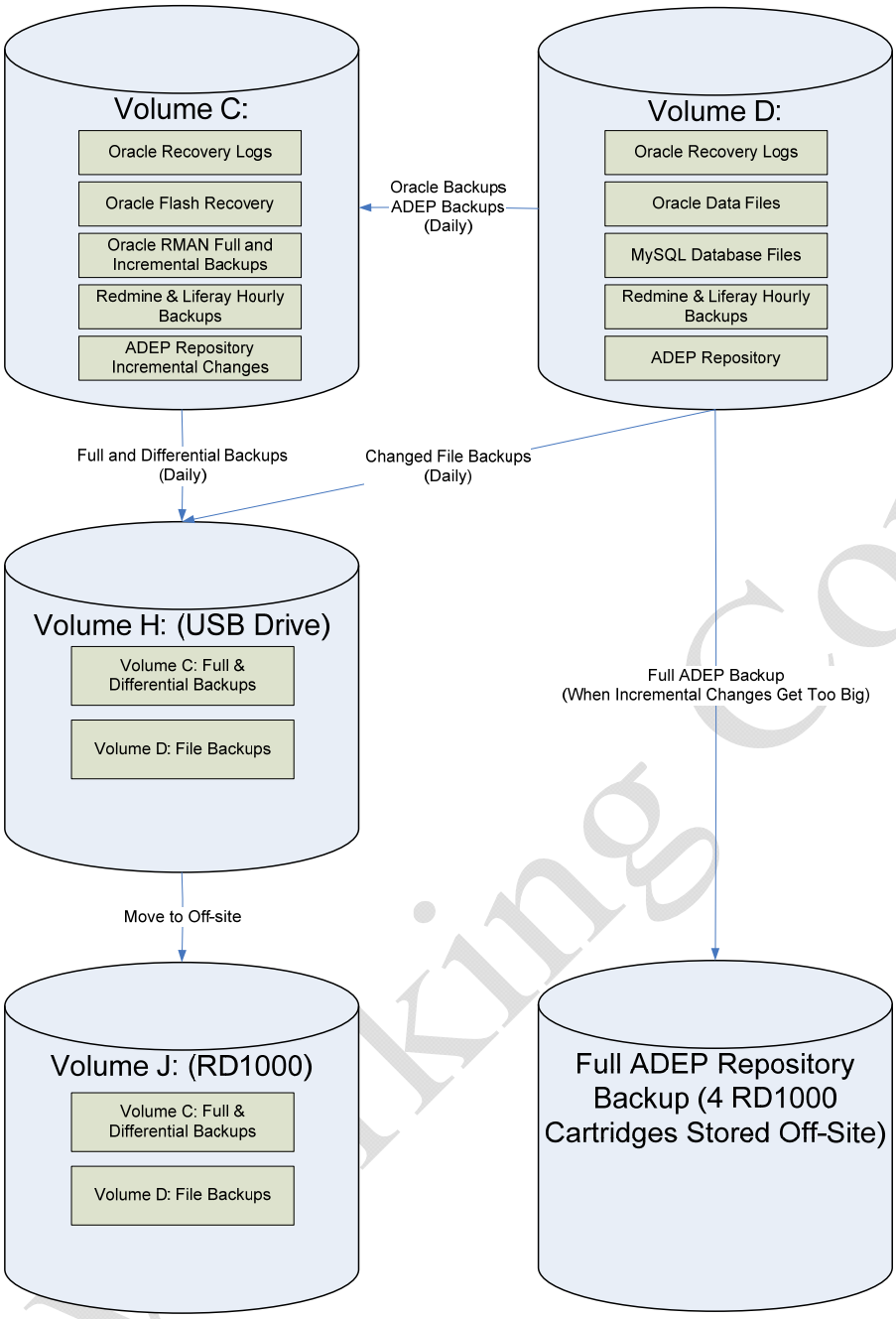


Figure 97. Schematic - Backup process overview.

Drive Backup Strategy

The RD1000 mounted on drive J: is used to write backups for off-site storage. The system uses 500GB cartridges for working off-site backups. 1 TB cartridges are used for backup of AIMS material. A 1 TB WD1000 external hard drive mounted on Drive M: is used for incremental backups.

There are multiple types of backups taking place. First, there are the drive level backups. Symantec Backup Exec System Recovery 2010 is used to back up drive C: to the staging area H:\SymantecRecoveryPoints. The backup of drive C: starts with a full image backup on Sunday at 10:30 PM with differential backups created at 10:30 PM Monday through Saturday. The staging area maintains two full image/differential backup sets. The Backup Exec software also takes care of copying the current week's backup files to drive J: to be moved off-site. This copy occurs as the full or differential backup completes. The backup of drive D: is handled differently since the backup media is not large enough to contain an image backup. Drive D: is backed up on a file by file basis to H:\SymantecRecoveryPoints\LTPPDPW using Symantec Backup Exec 2010. There are several directories that are excluded from the backups such as the ADEP repositories and the LTPP database instances. This backup is scheduled to run every day at 11:30 PM. The backup job does not automatically copy files to drive J: for off-site storage when complete. There is a Windows Task Scheduler job (CopyIncrementalFileBackupToCartridge) that copies the H:\SymantecRecoveryPoints\LTPPDPW directory to J:\LTPPDPW at 6:00 PM every day.

Application Backup Strategy

Because it may be desirable to recover application data at finer grained intervals than the recovery of an entire drive, many applications have their own backups being produced.

Oracle Database Instances

The control files and redo logs are written to drives D: and K:\ in \LTPP_Database\<instance> where <instance> is IMSProd, IMSTest, or IMSDev. The control files contain the latest structure of the database files and the redo logs contain the latest transactions. Drive K: contains the Flash Recovery Area in K:\LTPP_Database\<instance>\FlashRecoveryArea-and the Archive Logs in C:\LTPP_Database\<instance>\ArchiveLogs. If drive C: fails, drive D: contains all of the files necessary to recover the database. If drive D: fails, the RMAN backups from drive C:'s Flash Recovery Area will need to be restored and the logs applied in order to recover the database. Redo logs and archive logs are managed by the Oracle instance and allow recovery of the last transaction committed before the failure. The RMAN backups are managed by two Windows Task Scheduler jobs. The "RMAN Level 0 Backup" runs every Tuesday at 6:00 AM. This job produces a full backup of the instance and removes old archive logs and backup sets that are no longer necessary. The "RMAN Backup" runs every day at 10:00 PM. It produces a differential backup of changes to the data base instances. The drive C: backup captures these backups for off-site storage.

AIMS Repository and Historical Files

The AIMS Repository and historical files are too big to fit onto a single cartridge. As a complete copy of the AIMS exists on an external hard drive in the possession of Customer Service in addition to the copy on the DPW, the decision has been made not to backup video files. A full backup strategy has been implemented for all other files. The

AIMS repositories reside in K:\Historical_AIMS\<YYYY> where <YYYY> is year of the update. The backups are done the 1st Wednesday of February, May, August and November of each year and run for more than 24 hours due to the inclusion of the verify option in Symantec Backup Exec 2010.

Recovery Media

The CDs required to rebuild the server are located in server room in the top right drawer of the credenza. ~~They are in a brown accordion folder labeled DPW inside of a white Banker's Box that is in the center section of the credenza.~~ Return of off-site backups can be requested from First Federal Corporation. The information system owner would be the primary person to interface with First Federal Corporation. The system administrator would be the secondary contact.

Dell Service

The DPW server is a R515 with service tag ~~3WTNPQ1~~. It is covered by the "Gold or ProSupport with Mission Critical" and the "4 Hour On-Site Service" plans until ~~5/13/2014~~. These warranty plans ensure that the DPW will be repaired quickly. The system administrator would be the primary person to interface with Dell Support. The information system owner would be the secondary contact.

The two MD1000 25 TB storage units with service tags …. And ... are out of warranty. Necessary repairs are done by the system administrator.

Phase II: Activation

Decision Process

The decision to implement will begin with the initial notification that the server is not functioning. This will typically be on direct observation by the system administrator. Upon identification, the severity of the problem will be assessed. If it is determined that the problem can likely be resolved by a restart of services, then those actions will be taken before implementing this plan.

Alert and Notification

If it is determined that actions beyond a quick fix, the information system owner and the TSSC program manager will be notified in person, by phone or by e-mail as appropriate . This notification will include any details that are known about the outage along with an expected duration if it is known. This notice should be followed up with additional emails as details become available. Finally, notice should be sent when the system is available for use.

Phase III: Continuity Operations

Essential Functions

The essential function of data archival can continue with only a slight degradation. This is because the there are at least two other off-site copies of the information on the TFHRC server. Data extraction for general dissemination occurs during the August to November time frame which is the most critical period for on-line functionality. Down time primarily affects schedules in the extraction and review process. Data extraction on request is a process that occurs in low volumes sporadically throughout the year. Most responses are based on the Access® version of the database (standard data release – SDR) copied in quantity to USBs as part of the dissemination process and will not be impacted by downtime. The few requests that cannot be handled with the SDR require access to AIMS and can be addressed with the copy maintained by Customer Support. Downtime primarily affects turnaround time on a response.

Essential Personnel

- Order of Succession
    - System Administrator
    - Information Systems Owner
    - FHWA IT
- Delegation of Authority

Essential Equipment and Systems

- PowerEdge R515
- 2 MD1200 40TB storage units
- RD1000 External Cartridge Drive
- WD 1 TB External Hard Drive
- Connection to the internet
- Installation Media

Continuity Facilities

Resumption of operations in the event of a catastrophic failure at the TFHRC facility will follow the plan for the facility as a whole.

Continuity Communications

There is not another connection to the internet designated for resuming operations in the event of a catastrophic event at the TFHRC facility. Communications between personnel will be accomplished using a combination of phone and email.

Phase IV: Reconstruction Operations

The plan is to repair current systems to restore service. This will be accomplished using vendor support such as the Dell on-site service contract along with THFRC systems personnel to restore the THFRC server with the least data loss possible. When the THFRC is ready to be used for data dissemination, a notice will be sent to the contacts listed in the Alert and Notification section.

APPENDIX S. DISASTER RECOVERY – DPW

INTRODUCTION

Purpose

The purpose of the disaster recovery plan is to define a set of potential problems and their likely solution.

Planning Assumptions

The basic assumption is that there is a three day window to recover from a disaster without causing serious disruption in data dissemination capabilities. Given that a hot standby is not required, it has been decided that the most cost effective solution is to repair whatever is wrong with the current system and resume operations. We are counting on the Dell ProSupport Mission Critical Option that specifies 4 hour on-site service with 6 hour parts availability to resolve any hardware problems with the DPW. We are also counting on Iron Mountain to be able to deliver backups from off-site storage within three hours of an emergency request.

Objectives

The main objective is the restore the DPW to full operational status as soon as possible with minimal data loss. A secondary objective is to keep key personnel at the FHWA, and the TSSC informed about the problem and its resolution. When possible, limited functionality will be made available while permanent repairs are underway.

Concept of Operations

SYSTEMS OVERVIEW

The DPW has databases and files housed on a single server that is accessible either on location or via VPN. As shown in figure 98 a keyboard connected via a ?? switch and VPN are the primary entry points into the system.

Insert figure here.

Figure 98. Schematic. DPW server access diagram.

Risk Identification and Mitigation

Internet Connection Failure

- Description -An internet connection failure will first become apparent due to failure to access the system via VPN.

- Effect - The effect is that the server appears to be down for external access. There will be no remote connection capability. On the server side, everything is functioning normally and access will return as soon as the internet connection is restored.

- Mitigation - There are no workarounds to allow the user access to the server.

- Resolution - Notify FHWA IT that the VPN network is down. This step is typically unnecessary since they have automated notifications when the BPN network has a problem. Wait for service to be restored.

DPW Software Services Become Unresponsive

- Description - Software services becoming unresponsive typically results in inability to access an Oracle instance.

- Effect -The effect is that users are prevented from using the affected Oracle instance.

- Mitigation - No mitigation is necessary.

- Resolution - First use Process Explorer (procexp.exe) to see if there are any processes with high resource utilization. The resources to check are CPU, Disk I/O, and Memory. In normal operation, the CPU rarely exceeds 15%, the Commit Charge is rarely over 20 GB, and the Disk Bytes is typically under 100 KB/s. If a process is found to be causing the server to exceed these limits, determine if it needs to be killed or restarted.

  If resources were not the problem, check the following table to determine which service needs to be restarted. On rare occasions, a restart of the DPW may be required.

Table 13 - DPW service diagnostics.

Service	***Description***
OracleOraDb11g_home2TNSListener	This listens for connections to the Oracle database instances. Restart this service if having Oracle connection problems. Restarting this service will typically not impact users greatly. Restart takes about 30 seconds.
OracleServiceIMSDEV	This is the **development** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSPROD	This is the **production** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSTEST	This is the **test** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.

Single Hard Drive Failure on the RAID 1 Array

- Description - A single drive failure on the RAID 1 array (C:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.

- Effect - There is no effect on server operations.

- Mitigation - No mitigation is possible.

- Resolution - Contact Dell Support and declare this a severity 1 critical situation because if the other internal drive fails before the bad drive is replaced and had time to rebuild, the entire system volume is lost. This will cause the server to be unavailable until the drives are replaced and reloaded from backups.

  A 30 minute to 1 hour down time will be required to replace the failed drive when the replacement arrives. After the replacement, there could be a period of several hours where performance is degraded due to the mirror being rebuilt.

Single Hard Drive Failure on the RAID 5 Array

- Description - A single drive failure on the RAID 5 array (D:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.

- Effect - There is no effect on server operations.

- Mitigation - The hot spare will take the place of the failed drive. There are a few hours while the hot spare is being built where server performance may be degraded and the loss of an additional drive could cause the loss of the array.

- Resolution - Contact Dell and have them ship a replacement drive under warranty. When the replacement arrives, hot swap the failed drive and the replacement. The replacement drive will become part of the array and the hot spare will go back to its role as a standby. There may be a few hours of degraded performance while the replacement drive is being rebuilt.

Failure of the RAID 1 Array

- Description - A failure of the RAID 1 Array (C:) would take down the server. The system will not boot.

- Effect - Because the operating system is on C:, the system would not be able to continue operations and it would be impossible to reboot the server due to the lack of a boot drive.

- Mitigation - ~~A copy of the latest drive C: backup is kept on an attached USB drive as well as removable RD1000 cartridges.~~

- Resolution - Contact Dell and have them determine the cause of the failed array. After the failed drives and/or controllers are replaced, install the OS and Symantec Backup Exec 2010. From there, you can restore the latest usable backup. The Oracle instances will likely need recovery after drive C: is restored due to the sudden crash of the operating system. The expected downtime would be 1 to 2 days.

Failure of the RAID 5 Array

- Description - A failure of the RAID 5 Array (D:) would leave the server running, but the portals, Redmine, LTAS, APEX, and ADEP would be unavailable because they depend on database repositories on D:. The code repositories would still be accessible if needed.

- Effect - Files on D: will be unavailable. There will also be a loss of data due to some files not being backed to stay within the limitations of our backup media. The files that will be lost are not critical to operations.

- Mitigation - A copy of the latest drive D: backup is kept on an attached USB drive as well as removable RD1000 cartridges.

- Resolution - Contact Dell and have them determine the cause of the failed array. After the failed drives and/or controllers are replaced, copy the files from the latest backup onto the D: drive. It will also be necessary to have the four cartridges that make up ADEP backup returned from Iron Mountain off-site storage. The contents of those cartridges will need to be copied onto D: and then the incremental backups from drive C: will need to be applied to restore ADEP to a point that is within 1 day of the crash. The Oracle database instances will need to be restored from the RMAN backups on C: and the logs applied to roll the databases forward until the point that the Array failed. If for some reason the MySQL instance does not come up, it can be recreated using the backups located in C:\backup. The expected downtime would be 2 to 3 days. Most services could be restored by the second day with ADEP being the last service to come back online.

Complete Loss of Facilities at Oak Ridge

- Description - This would be a catastrophic event that completely destroys the facilities at Oak Ridge along with the server and on-site backups.

- Effect - No services provided by the DPW server would be available.

- Mitigation - Off-site backups stored outside of Oak Ridge.

- Resolution - The latest off-site backups would be shipped to Oak Ridge where the external RD1000 drive could be used to apply the backups to a Windows 2008 R2

server built in the Amazon cloud. The Internet Protocol (IP) address of the portals would be redirected to the IP address of the Amazon hosted server. The expected downtime would be approximately a week. This largely depends on how long it takes to set up an LTPP account on Amazon and how long it takes to transfer the backup data into the cloud storage.

APPENDIX T. REFERENCE DOCUMENTS

DATA USER GUIDES

LTPP IMS User Guide

The Long-Term Pavement Performance Information Management System User Guide (User Guide) gives the user an in-depth look at all of the data modules and most of the tables in the Pavement Performance Database. As of SDR 28 the document included information on LTAS and AIMS. This document should be the data analyst's best friend. The version distributed with SDR 29 is located in the Reference Document subdirectory. (*User_Guide_2013.pdf*)

QC Manual

This manual documents the QC checks to which the LTPP data is subject through the QC programs. The last distributed version is dated *September 2013* and can be found in the Reference Documents subdirectory. (*QCMan2013.pdf*)

Accessing LTPP Data

This document is intended to provide tips to Microsoft Access® users on how to effectively use Access to analyze LTPP data. It includes Access tips and tricks and tidbits about the LTPP data. The most recent version of this document is in the Reference Documents subdirectory. (*Accessing_LTPP_Data_2013.pdf*)

LTAS User Guide/Bookshelf

The 2010 version of the LTAS User Guide can be found in the Reference Documents subdirectory. (Analysis Vol_1-0_2010_05_26.pdf) In addition, a description of other LTAS documentation is included in the LTAS Bookshelf (LTPP_Traffic_Bookshelf_2006_05_25.pdf). Current versions of these documents can be requested from LTPP Customer Support.

OPERATIONS

IT Security

Data Repository Server IT Security Plan for the Long Term Pavement Performance Program, December 2013.

Hardware Manuals

Dell PowerEdge R515 - http://www.dell.com/support/home/us/en/19/product-support/servicetag/5XT8H02/manuals, accessed 5/6/2015.

DELL PowerEdge 2900 – http://www.dell.com/support/home/us/en/19/product-support/product/poweredge-2900/manuals, accessed 5/4/2015.

DELL PowerVault MD1000 – http://www.dell.com/support/home/us/en/04/product-support/product/powervault-md1000/manuals, accessed 5/8/2015.

DELL PowerVault MD1200 – http://www.dell.com/support/home/us/en/04/product-support/product/powervault-md1200/manuals, accessed 5/7/2015.

APC Smart UPS 2200 DLA Model -

APC Smart UPS 2200 SMT Model - http://www.apcmedia.com/salestools/MMIS-8HUQQZ/MMIS-8HUQQZ_R2_EN.pdf?sdirect=true accessed 5/7/2015.

Software Manuals

Symantec Backup Exec 2015 -

Symantec Backup Exec 2010 R2 – http://www.symantec.com/business/support/index?page=content&id=DOC2211, accessed 12/17/201.3

APEX – Version 4.2.5.00.8 was current on the DPW as of 5/7/2015. For the most current documentation see http://www.oracle.com/technetwork/developer-tools/apex/documentation/index.html which may require a free account on Oracle Technology Network. *http://docs.oracle.com/cd/E17556_01/doc/user.40/e15517.pdf, Oracle® Application Express, Application Builder User's Guide, Release 4.0, E15517-02, September 2010, accessed 12/17/2013.*

SQL Developer – http://www.oracle.com/technetwork/developer-tools/sql-developer/documentation/documentation-index-152579.html accessed 5/7/2015 is the index to all SQL Developer documentation. Version installed as of 5/7/2015 is 4.0.3 on the TFHRC server and ... *on the Dell 2900.*

Notepad++ - notepad-plus-plus.org, accessed 5/7/2015. There is no user documentation per se but references and links to support.

Long-Term Pavement Performance Data entry Portal (LDEP) User Guide, November 2012.

Source Code Inventory

This document was created to give an inventory of all source code developed at SAIC in the course of working on the LTPP contracts since 1989. The source code is kept in a configuration management system (PVCS) that is organized by logical groupings of programs. The Table of Contents mirrors this directory structure. Individual programs are listed in the body of the document in its respective group. *For example, QC programs are written in Pro-C, so they are in the IMS\PC\QC directory.* The last hard copy of this document was created in 2010. The current inventory is kept in Tortoise

SVN, a type of version control software. The version of each software package and utility developed by the LTPP program current and in use at the time of the SDR is provided for storage and backup at TFHRC under K:\... after the submission of the SDR on the Dell 2900. The same files are stored on the *TFHRC server under …*

SPR Database

The SPR Database is an Access database that has all SPRs from mid-1993 to August 2011. Earlier SPRs were kept in hardcopy and are now in electronic form for easy searching. The SPR Database includes dates that the SPR was received, referred, and completed; it includes a description and a resolution; and it includes the originating organization. Several reports are available from the Access Reports list.

SPRs since that date are maintained in a Redmine project accessible to users of the DPW.

Directive I-170

This document provides information about AIMS electronic data format and submission standards. *It is located in the Reference Documents directory, I-170.pdf, along with the first amendment, . Dates for AIMS updates are contained in directive ??? or its replacements.*

APPENDIX AA. ROLES AND RESPONSIBILITIES – DELL 2900

The Disaster Recovery (DR) and Continuity of Operations Plan (COOP) appendices along with the "Data Processing Workstation IT Security Plan for the Long Term Pavement Performance Program" require that persons be identified to fulfill various roles. This section describes the roles required and the organizations providing individuals for those roles. The assignment of individuals by role and their contact information is provided by quarterly memo to the COR who is the Information System Owner. The contact information for the various organizations and individuals is also included. The information is provided separately from this document to remove personally identifiable information (PII) and prevent obsolescence of this document.

The role assignments for this system are reviewed quarterly. The organizations with people assigned to each role are documented in table 14. Contact information for each organization is provided in table 15.

- System Administrator - The system administrator is responsible for maintaining the Dell 2900 in good working order. This includes the operating system, access control, installed software, backups, and hardware.

- Backup System Administrator - The backup system administrator is responsible for maintaining the Dell 2900 under the direction of the system administrator and/or when the system administrator is unavailable. This includes the operating system, access control, installed software, backups, and hardware.

- Dell 2900 Database Administrator - The database administrator maintains the database instances on the Dell 2900. This includes database backups, schema modification, and storage management.

- Backup Dell 2900 Database Administrator - The backup database administrator maintains the database instances on the Dell 2900. This includes database backups, schema modification, and storage management under the direction of the database administrator and/or when the database administrator is unavailable.

- TSSC Program Manager - The TSSC program manager is responsible for the oversight of the LTPP server activities at TFHRC.

- Technical Support Services Staff - The technical support services staff role provides support for LTPP server activities on-site under supervision of the Dell 2900 database administrator.

- Customer Service - The Customer Service role is responsible for answering customer inquiries including distributing data. Customer Service is also responsible for maintaining some centrally processed data and maintaining copies of ADEP on the Dell 2900 server.

- TFHRC IT – The TFHRC IT role is responsible for maintenance of FHWA supplied operating and anti-virus software and supporting hardware maintenance activities.

- Information System Owner - The information system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the system.

- Authorizing Official - The authorizing is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

- Assignment Of Security Responsibility - The assignment of security responsibility role is responsible for the overall security of the Dell 2900.

- Other Designated Contacts - The other designated contacts role designates key contact personnel who can address inquiries regarding system characteristics and operation.

- LTPP - The LTPP role provides FHWA oversight of the LTPP program.

Table 14. TFHRC Server Role Assignments

Role	Organization with Individuals in the Role
System Administrator	AMEC
Backup System Administrator	SAIC
TFHRC Database Administrator	AMEC
Backup TFHRC Database Administrator	SAIC
TSSC Program Manager	AMEC
Customer Service User	ESCINC
Technical Support Services Staff	AMEC
Information System Owner	FHWA
Authorizing Official	FHWA
Assignment Of Security Responsibility	AMEC
Other Designated Contacts	None
LTPP	See Team listing[1]
FHWA IT	TFHRC Help Desk

[1] http://www.fhwa.dot.gov/research/tfhrc/programs/infrastructure/pavements/ltpp/whoswho.cfm

Table 15. Dell 2900 Server - Organizational Contact Information

Organization	Contact Information
Long Term Pavement Program Team (LTPP):	FHWA/DOT, HRDI-30 6300 Georgetown Pike McLean, VA 22101

Organization	Contact Information
TFHRC IT:	FHWA/DOT, HRRM-1 6300 Georgetown Pike McLean, VA 22101
SAIC:	151 Lafayette Drive Oak Ridge, TN 37830
AMEC Environment & Infrastructure (AMEC):	12000 Indian Creek Court, Suite F Beltsville, MD 20705 (301) 210-5105
Engineering & Software Consultants, Inc. (ESCINC)	14123 Robert Paris Court Chantilly, VA 20151

APPENDIX AB. CONTINUITY OF OPERATIONS – DELL 2900

PURPOSE

The Continuity of Operations Plan (COOP) describes how the Long Term Pavement Performance (LTPP) Program will continue to function when the Dell 2900 server is unable to sustain normal operations. The outage may be partial or total and may be the result of operator error, software problems, hardware problems, or network connectivity problems.

Scope

The scope of this COOP is the Dell 2900 Server.

Situation Overview

The Dell 2900 is used for parallel processing of the central archival of data gathered by the regional contractors. It provides a back up for data disseminated to the public through on demand requests. Original copies of the data are maintained on the DPW and within the regions. Because the original data is not lost, it is possible for the Dell 2900 server to be unavailable for a period of time without causing all data dissemination activity to stop. The primary risk to the system being unavailable is that failure of both servers may halt cusstom data dissemination.

Planning Assumptions

The LTPP Team has agreed that two weeks of downtime would not have an adverse effect on data delivery for this parallel system. It has also been decided that if a hardware problem occurs with the server, server repairs will be contingent on the expected remaining time for parallel processing and cost. Therefore there is not a failover system standing by. As explained later, we will rely on TFHRC's Help Desk to support repair of the system in the event of a hardware failure.

Objectives

The objective of this plan is to outline the steps necessary to minimize disruption to LTPP data delivery in case of a system failure.

CONCEPT OF OPERATIONS

Phase I: Readiness and Preparedness

Knowing that system failures are inevitable, there are certain steps that can be taken ahead of time to ensure that services can be restored in a timely manner.

Backups

The server contains two Redundant Array of Independent Disks (RAID) volumes. The first volume is configured as a RAID 1 array consisting of two 1 TB Serial-Attached Small Computer System Interface (SAS) drives. This volume is the C: drive and contains the operating system as well as a copy of the database backups, source code repository, and archive logs. This drive also hosts the bulk of the web applications. The RAID 1 array can withstand a single drive failure and remain operational. These drives are not hot swappable. The second volume is configured as a RAID 5 array consisting of seven 2 TB SAS drives. There is an eighth 2 TB SAS drive standing by as a hot spare. This array can withstand a single drive failure and the hot spare will automatically take the place of the failed drive providing additional protection until the failed drive can be replaced. These drives are hot swappable. This array is the D: drive and contains the database instances, ADEP repositories, and backup staging areas.

The schematic in Figure 100 below shows the highlights of the backup process.

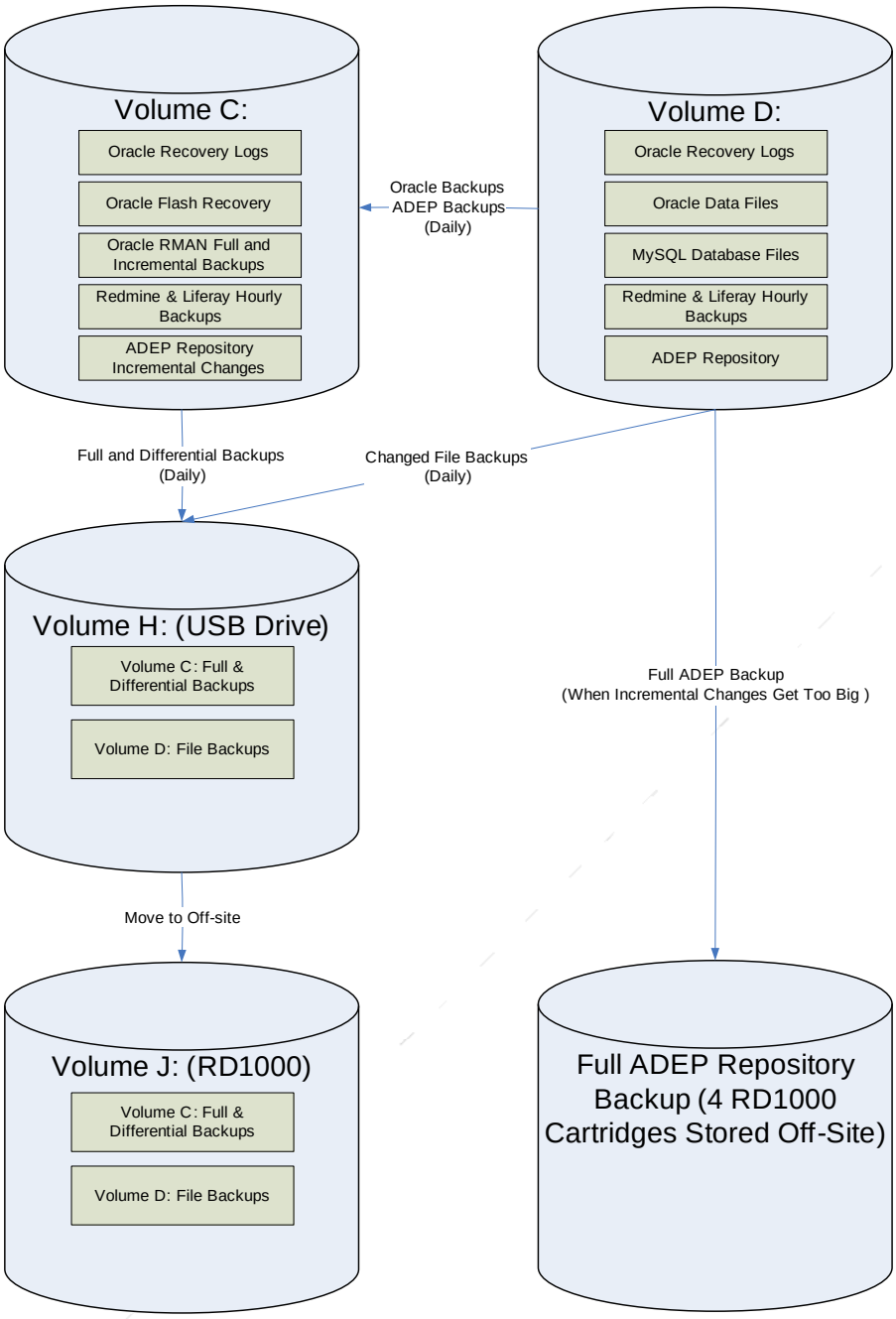


Figure 99. Schematic - Backup Process Overview – Replace with Dell 2900 equivalent.

Drive Backup Strategy

The RD1000 mounted on *drive J: is* used to write backups for off-site storage. The system uses 500GB cartridges for working off-site backups. 1 TB cartridges are used for backup of AIMS material. A 1 TB WD1000 external hard drive mounted on *Drive M:* is used for incremental backups.

There are multiple types of backups taking place. *First, there are the drive level backups. Symantec Backup Exec System Recovery 2010 is used to back up drive C: to the staging area H:\SymantecRecoveryPoints. The backup of drive C: starts with a full image backup on Sunday at 10:30 PM with differential backups created at 10:30 PM Monday through Saturday. The staging area maintains two full image/differential backup sets. The Backup Exec software also takes care of copying the current week's backup files to drive J: to be moved off-site. This copy occurs as the full or differential backup completes. The backup of drive D: is handled differently since the backup media is not large enough to contain an image backup. Drive D: is backed up on a file by file basis to H:\SymantecRecoveryPoints\LTPPDPW using Symantec Backup Exec 2010. There are several directories that are excluded from the backups such as the ADEP repositories and the LTPP database instances. This backup is scheduled to run every day at 11:30 PM. The backup job does not automatically copy files to drive J: for off-site storage when complete. There is a Windows Task Scheduler job (CopyIncrementalFileBackupToCartridge) that copies the H:\SymantecRecoveryPoints\LTPPDPW directory to J:\LTPPDPW at 6:00 PM every day.*

Application Backup Strategy

There are no applications on the Dell 2900 beyond the Oracle databases that require application specific backups.

Oracle Database Instances

The control files and redo logs are written to drives D: and K:\ in \LTPP_Database\<instance> where <instance> is IMSProd, IMSTest, or IMSDev. The control files contain the latest structure of the database files and the redo logs contain the latest transactions. Drive K: contains the Flash Recovery Area in K:\LTPP_Database\<instance>\FlashRecoveryArea and the Archive Logs in C:\LTPP_Database\<instance>\ArchiveLogs. If drive C: fails, drive D: contains all of the files necessary to recover the database. If drive D: fails, the RMAN backups from drive C:'s Flash Recovery Area will need to be restored and the logs applied in order to recover the database. Redo logs and archive logs are managed by the Oracle instance and allow recovery of the last transaction committed before the failure. The RMAN backups are managed by two Windows Task Scheduler jobs. The "RMAN Level 0 Backup" runs every Tuesday at 6:00 AM. This job produces a full backup of the instance and removes old archive logs and backup sets that are no longer necessary. The "RMAN Backup" runs every day at 10:00 PM. It produces a differential backup of changes to the data base instances. The drive C: backup captures these backups for off-site storage.

AIMS Repository and Historical Files

The AIMS Repository and historical files are too big to fit onto a single cartridge. As a complete copy of the AIMS exists on an external hard drive in the possession of Customer Service in addition to the copy on the DPW, the decision has been made not to backup video files. A full backup strategy has been implemented for all other files. The

AIMS repositories reside in K:\Historical_AIMS\<YYYY> where <YYYY> is year of the update. The backups are done the 1st Wednesday of February, May, August and November of each year and run for more than 24 hours due to the inclusion of the verify option in Symantec Backup Exec 2010.

Recovery Media

The CDs required to rebuild the server are located in server room in the top right drawer of the credenza. They are in a brown accordion folder labeled DPW inside of a white Banker's Box that is in the center section of the credenza. Return of off-site backups can be requested from First Federal Corporation. The information system owner would be the primary person to interface with First Federal Corporation. The system administrator would be the secondary contact.

Dell Service

The Dell PowerEdge 2900 is out of warranty. The two MD1000 25 TB storage units are out of warranty. Necessary repairs are done by the system administrator with support from FHWA and TFHRC IT support.

Phase II: Activation

Decision Process

The decision to implement will begin with the initial notification that the Dell 2900 is not functioning. This will typically be on direct observation by the system administrator. Upon identification, the severity of the problem will be assessed. If it is determined that the problem can likely be resolved by a restart of services, then those actions will be taken before implementing this plan.

Alert and Notification

If it is determined that actions beyond a quick fix, the information system owner and the TSSC program manager will be notified in person, by phone or by e-mail as appropriate. This notification will include any details that are known about the outage along with an expected duration if it is known. This notice should be followed up with additional emails as details become available. Finally, notice should be sent when the system is available for use.

Phase III: Continuity Operations

Essential Functions

The essential function of data archival can continue with only a slight degradation. This is because the there are at least two other off-site copies of the information on the Dell 2900. Data extraction for general dissemination occurs during the March and April time frame which is the most critical period for on-line functionality. Down time primarily affects schedules in the extraction and review process. Data extraction on request is a

process that occurs in low volumes sporadically throughout the year. Most responses are based on the Access® version of the database (standard data release – SDR) or use of Infopave. The few requests that cannot be handled with the SDR require access to AIMS and can be addressed with the copy maintained by Customer Support. Downtime primarily affects turnaround time on a response.

Essential Personnel

- Order of Succession
    - System Administrator
    - Information Systems Owner
    - FHWA IT
- Delegation of Authority

Essential Equipment and Systems

- PowerEdge 2900 (TFHRC Server)
- 2 MD1000 25 TB storage units
- RD1000 External Cartridge Drive
- WD 1 TB External Hard Drive
- Connection to the internet
- Installation Media

Continuity Facilities

Resumption of operations in the event of a catastrophic failure at the TFHRC facility will follow the plan for the facility as a whole.

Continuity Communications

There is not another connection to the internet designated for resuming operations in the event of a catastrophic event at the TFHRC facility. Communications between personnel will be accomplished using a combination of phone and email.

Phase IV: Reconstruction Operations

The plan is to repair the Dell 2900 system to the extent needed to support parallel processing. This will be accomplished using THFRC systems personnel to restore the Dell 2900 with the least data loss possible. When the Dell 2900 is ready to be used for

data dissemination, a notice will be sent to the contacts listed in the Alert and Notification section.

APPENDIX AC. DISASTER RECOVERY – DELL 2900

INTRODUCTION

Purpose

The purpose of the disaster recovery plan is to define a set of potential problems and their likely solution.

Planning Assumptions

The basic assumption is that there is a two week window to recover from a disaster without causing serious disruption in data dissemination capabilities. Given that a hot standby is not required, it has been decided that the most cost effective solution is to repair whatever is wrong with the Dell 2900 and resume operations. We are counting on internal TFHRC resources to resolve hardware and OS issues. We are also counting on First Federal Corporation to be able to deliver backups from off-site storage within forty-eight hours of an emergency request.

Objectives

The main objective is the restore the Dell 2900 to full operational status as soon as possible with minimal data loss. A secondary objective is to keep key personnel at the FHWA, and the TSSC informed about the problem and its resolution. When possible, limited functionality will be made available while permanent repairs are underway.

Concept of Operations

SYSTEMS OVERVIEW

The Dell 2900 has databases and files housed on a single server that is accessible either on location or via VPN. As shown in Figure 100 a keyboard connected via a KVN switch and VPN are the primary entry points into the system.

Insert figure here.

Figure 100. Schematic. TFHRC Server Access Diagram

Risk Identification and Mitigation

Internet Connection Failure

Not applicable. This unit is not longer on the list of machines approved by TFHRC IT for internet access.

Dell 2900 Software Services Become Unresponsive

- Description - Software services becoming unresponsive typically results in inability to access an Oracle instance.

- Effect -The effect is that users are prevented from using the affected Oracle instance.

- Mitigation - No mitigation is necessary.

- Resolution - *First use Process Explorer (procexp.exe) to see if there are any processes with high resource utilization. The resources to check are CPU, Disk I/O, and Memory. In normal operation, the CPU rarely exceeds 15%, the Commit Charge is rarely over 20 GB, and the Disk Bytes is typically under 100 KB/s. If a process is found to be causing the server to exceed these limits, determine if it needs to be killed or restarted.*

  If resources were not the problem, check the following table to determine which service needs to be restarted. On rare occasions, a restart of the Dell 2900 may be required.

Table 16. Dell 2900 Service Diagnostics.

Service	***Description***
OracleOraDb11g_home2TNSListener	This listens for connections to the Oracle database instances. Restart this service if having Oracle connection problems. Restarting this service will typically not impact users greatly. Restart takes about 30 seconds.
OracleServiceIMSDEV	This is the **development** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSPROD	This is the **production** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.
OracleServiceIMSTEST	This is the **test** instance of Oracle. Restart this service if Oracle is not responding. This service typically takes about two minutes to restart. This service may not restart after completion of backups or restarts following Windows software updates. It is likely that a problem requiring the restart of this service may also require applying redo logs to bring the instance to a consistent state.

Single Hard Drive Failure on the RAID 1 Array

- Description - A single drive failure on the RAID 1 array (C:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.

- Effect - There is no effect on server operations.

- Mitigation - No mitigation is possible.

- Resolution - Replace the hard drive immediately using the drive on hand. If a drive must be purchased, failure of the second drive may result in having to do a complete rebuild from backups.

  A 30 minute to 1 hour down time will be required to replace the failed drive when the replacement arrives. After the replacement, there could be a period of several hours where performance is degraded due to the mirror being rebuilt.

Single Hard Drive Failure on the RAID 5 Array

- Description - A single drive failure on the RAID 5 array (D:) will not be evident other than by using Dell's Server Administrator or seeing status lights on the server.

- Effect - There is no effect on server operations.

- Mitigation - The hot spare will take the place of the failed drive. There are a few hours while the hot spare is being built where server performance may be degraded and the loss of an additional drive could cause the loss of the array.

- Resolution – Purchase a replacement drive. When the replacement arrives, hot swap the failed drive and the replacement. The replacement drive will become part of the array and the hot spare will go back to its role as a standby. There may be a few hours of degraded performance while the replacement drive is being rebuilt.

Failure of the RAID 1 Array

- Description - A failure of the RAID 1 Array (C:) would take down the server. The system will not boot.

- Effect - Because the operating system is on C:, the system would not be able to continue operations and it would be impossible to reboot the server due to the lack of a boot drive.

- Mitigation - *A copy of the latest drive C: backup is kept on an attached USB drive as well as removable RD1000 cartridges.*

- Resolution - Contact TFHRC IT and have them determine the cause of the failed array. After the failed drives and/or controllers are replaced, install the OS and

Symantec Backup Exec 2010. From there, restore the latest usable backup. The Oracle instances will likely need recovery after drive C: is restored due to the sudden crash of the operating system. The expected downtime would be 1 to 2 days.

Failure of the RAID 5 Array

- Description - *A failure of the RAID 5 Array (D:) would leave the server running, but the portals, Redmine, LTAS, APEX, and ADEP would be unavailable because they depend on database repositories on D:. The code repositories would still be accessible if needed.*

- Effect - *Files on D: will be unavailable. There will also be a loss of data due to some files not being backed to stay within the limitations of our backup media. The files that will be lost are not critical to operations.*

- Mitigation - *A copy of the latest drive D: backup is kept on an attached USB drive as well as removable RD1000 cartridges.*

- Resolution - *Contact TFHRC IT to determine the cause of the failed array. After the failed drives and/or controllers are replaced, copy the files from the latest backup onto the D: drive. The Oracle database instances will need to be restored from the RMAN backups on C: and the logs applied to roll the databases forward until the point that the Array failed. The expected downtime would be 2 to 3 days.*

Complete Loss of Facilities at TFHRC

- Description - This would be a catastrophic event that completely destroys the facilities at TFHRC along with the server and on-site backups.

- Effect - No services provided by the Dell 2900 would be available.

- Mitigation - Off-site backups stored outside of TFHRC.

- Resolution - The latest off-site backups would be shipped to TFHRC where the external RD1000 drive could be used to apply the backups to a Windows 2008 R2 server built in the Amazon cloud. The expected downtime would be approximately a week. This largely depends on how long it takes to set up an LTPP account on Amazon and how long it takes to transfer the backup data into the cloud storage.

APPENDIX AD. HARDWARE, SOFTWARE AND MAINTENANCE – DELL 2900

The original central server was purchased in April of 2009. The central server was purchased with the vision to be a central repository located at a FHWA facility instead of contractor facilities. It is located at FHWA's research facility, TFHRC, in McLean, VA. It is a Dell 2900 running Windows Server 2008. This server became the central server when operations were centralized at FHWA in the fall of 2009. Additional storage in the form of two MD1000 units was added in 2011. The server was replaced in 2015 but not inactivated.

The server is also designed to be somewhat fault tolerant. It features multiple power supplies and hot swappable hard drives. While the uptime requirements of the LTPP server are not that high, this redundancy helps to keep the systems running while waiting on parts to arrive. On the down side, without someone checking the system for faults on a regular basis, the servers can keep running for a long time with failed parts. This can lead to a loss of data if, for example, one hard drive has already failed and another fails before the first failure is repaired.

The hard drives are joined together in a single RAID 5 array. The hard drives are partitioned into volumes and these volumes are set aside for different purposes. Microsoft Windows Server is installed on the C: volume. The Oracle database files are stored on the D: volume.

When setting up the server, the operating system and various utilities such as the backup software were installed. Then the Oracle database software was installed and the database instances created.

The Dell 2900 server has had Microsoft Office loaded in order to be able to use Microsoft Access to process standard data releases. In addition Symantec Anti-virus, Symantec Backup Exec 2010, Adobe Acrobat, SQL Developer, Notepad++ and Tortoise SVN have been installed.

HARDWARE

The original central server is a Dell PowerEdge 2900 with two 3 GHz Xenon E5450 quad-core processors. This server also has 32 GB of RAM, an internal RAID 5 Array consisting of eight 7,200 RPM 1-TB SATA disks and an external RAID 5 Array consisting of thirty 5,400 RPM 2-TB SATA disks. For backups, it has a PowerVault RD1000 which accepts 1-TB hard disk cartridges and a ….*for incremental backups.* All of this is protected by a 2200 VA UPS.

Server Setup

The server setup for the Dell 2900 is detailed in HRD-LTPPServerSetup200906-1.doc (see Appendix T. Reference Documents.) This document describes in detail how the RAID Array, operating system and Oracle databases were configured. The highlights of the server setup are as follows:

The server was delivered with the Windows Server 2008 Operating System. This was then configured to comply with NIST 800-53 Revision 2 Annex 1 since this is a low impact system.

The server was originally made the DHCP and DNS server for the private LAN to which it is attached. There is no domain controller on this network. When the server was connected to the TFHRC Internet 2 network through IP6 it was no longer on a private network. The DHCP and DNS options were disabled.

Oracle 10g 10.2.0.4, which was the first version that handles 64-bit databases under Windows Server 2008, was originally installed on the server. When the DPW was activated, the central server was upgraded to Oracle 11g (11.2.0).

Once Oracle was installed, the production database instances (IMSProd and TRFProd) were created. After the production instances were created, two test instances (IMSTest, TRFTest) and two development instances (IMSDev, TRFDev) were cloned. The TRF instances were shut down after the LTAS instances were migrated to the PPDB.

Backups

The original central server uses Symantec Backup Exec and RD1000 500GB and RD1000 1TB Disk cartridges for backups.

The backup strategy is regular backups of the Oracle database to removable media. Due to the fact that major data changes are made quarterly and the other modifications are typically queries rather than modifications, a bi-weekly backup to removable media has been chosen as the proper balance between risk and cost for the central server. Incremental backups are performed on alternate days rather than daily.

The following guidelines are provided to assist in checking the Dell 2900 for problems before they result in data loss. It is recommended that these checks be performed on a weekly basis, concurrent with the server backup process.

Server status

Software inspection can be accomplished by using the Dell Remote Access Card (DRAC)- discuss basics. Since the physical inspection outlined in the following sections is usually sufficient, there is really no need to perform an inspection using the DRAC. All of the relevant messages will appear on the LCD panel.

The Hard Drives, Power Supplies, and the messages on the LCD panel should be checked once a week. A convenient time to perform this inspection is during backups since someone has to be physically at the server to mount the backup cartridge.

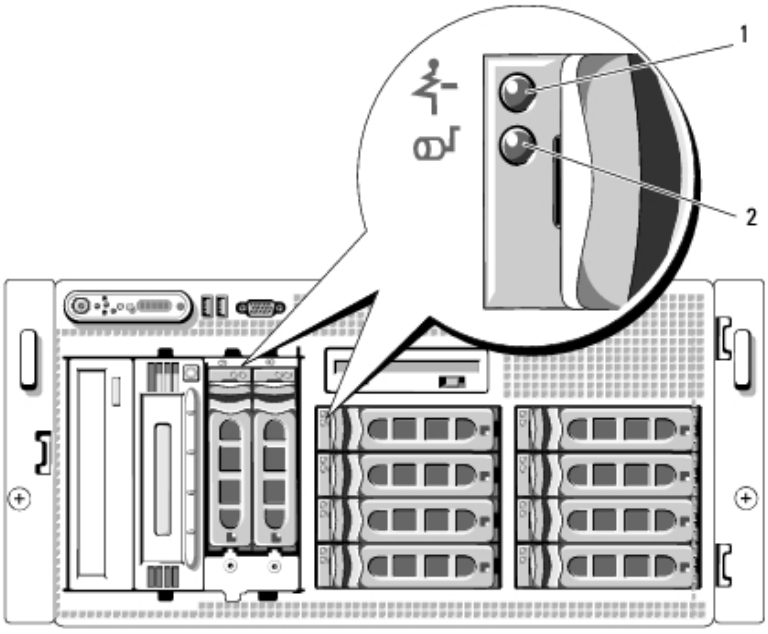
The following sections contain excerpts from the Dell™ PowerEdge™ 2900 Hardware Owner's Manual[11]. A copy of the manual is included in the reference documents folder accompanying this document.

The basic procedure is to look for lights that are amber. Each power supply should have a green power supply status and a green AC status indicator. And as a general check, the LCD panel in front should be lit with a blue light. If anything goes wrong on the system, the LCD panel will have an amber light which means further action is necessary.

Hard Drive Inspection

Figure 101 shows where the hard drive carriers may be on the front of the Dell 2900. The LTPP unit only has eight horizontal drives. The vertical drives in the illustration and all of the drives for removable media except for the DVD drive at the far left of the unit are not part of the LTPP system.

The hard-drive carriers have two indicators — the drive-status indicator and the drive-activity indicator (Figure 101). Each hard drive should have a green drive-status indicator.



[11] http://www.dell.com/support/home/us/en/19/product-support/product/poweredge-2900/manuals, accessed 5/7/2015.

1	drive-status indicator (green and amber)	2	green drive-activity indicator

Figure 101. Illustration[12]. Drive Status Indicators.

Table 17 lists the drive indicator patterns. Different patterns are displayed as drive events occur in the system. For example, if a hard drive fails, the "drive failed" pattern appears. After the drive is selected for removal, the "drive being prepared for removal" pattern appears, followed by the "drive ready for insertion or removal" pattern. After the replacement drive is installed, the "drive being prepared for operation" pattern appears, followed by the "drive online" pattern.

Table 17. Hard-drive indicator patterns.

Condition	Drive-Status Indicator Pattern
Identify drive/preparing for removal	Blinks green two times per second
Drive ready for insertion or removal	Off
Drive predicted failure	Blinks green, amber, and off.
Drive failed	Blinks amber four times per second.
Drive rebuilding	Blinks green slowly.
Drive online	Steady green.
Rebuild aborted	Blinks green three seconds, amber three seconds, and off six seconds.

Power Supply Inspection

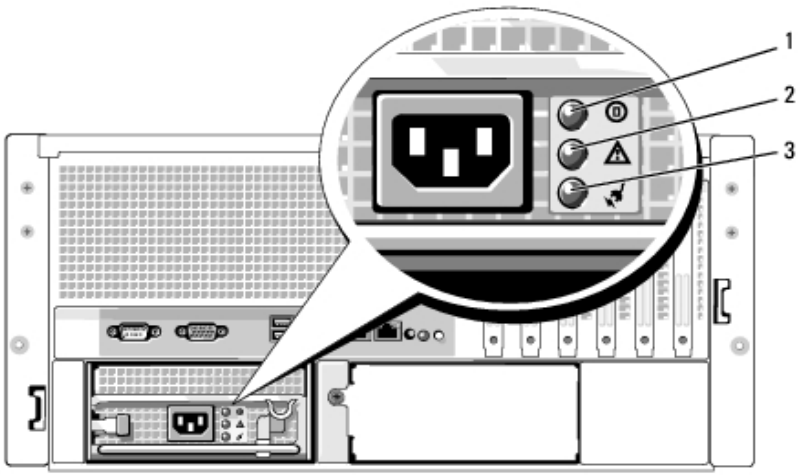
The power button on the front panel controls the power input to the system's power supplies. The power indicator lights green when the system is on.

The indicators on the optional redundant power supplies show whether power is present or whether a power fault has occurred (see table 18 and figure 102).

Table 18. Function of redundant power supply indicators.

Indicator	Function
Power supply status	Green indicates that the power supply is operational.
Power supply fault	Amber indicates a problem with the power supply.
AC line status	Green indicates that a valid AC source is connected to the power supply.

[12] Image taken from *Dell™ PowerEdge™ 2900 Systems Hardware Owner's Manual*.



1	power supply status	2	power supply fault	3	AC line status

Figure 102. Illustration[12]. Location of redundant power supply indicators.

LCD Status Messages

The system's control panel LCD provides status messages to signify when the system is operating correctly or when the system needs attention. The LCD lights blue to indicate a normal operating condition and lights amber to indicate an error condition. The LCD scrolls a message that includes a status code followed by descriptive text. The codes can be interpreted in more detail using Table 1-6 (page 18) of the *Dell™ PowerEdge™ 2900 Systems Hardware Owner's Manual*[11].

Server Troubleshooting

Troubleshooting for the Dell Poweredge 2900 consists of checking that all hard drives are working and knowledge of the possible error conditions for the system. The corrective actions references in table 19 apply to the sections of the hardware user's guide.

Table 19. Dell Poweredge 2900 LCD status message key.

Code	Text	Causes	Corrective Actions
N/A	*SYSTEM NAME*	A 62-character string that can be defined by the user in the System Setup program. The *SYSTEM NAME* displays under the following conditions: The system is powered on. The power is off and active POST errors are displayed.	This message is for information only. You can change the system string in the System Setup program. See Using the System Setup Program.
E1000	FAILSAFE, Call Support		See Getting Help.

Code	Text	Causes	Corrective Actions
E1114	Temp Ambient	Ambient system temperature is out of acceptable range.	See Troubleshooting System Cooling Problems.
E1116	Temp Memory	Memory has exceeded acceptable temperature and has been disabled to prevent damage to the components.	See Troubleshooting System Cooling Problems.
E1210	CMOS Batt	CMOS battery is missing, or the voltage is out of acceptable range.	See Troubleshooting the System Battery.
E1211	ROMB Batt	RAID battery is either missing, bad, or unable to recharge due to thermal issues.	Reseat the RAID battery. See Replacing the SAS RAID Controller Daughter Card Battery, and Troubleshooting System Cooling Problems.
E12*nn*	*XX* PwrGd	Specified voltage regulator has failed.	See Getting Help.
E1229	CPU # VCORE	Processor # VCORE voltage regulator has failed.	See Getting Help.
E1310	RPM Fan ##	RPM of specified cooling fan is out of acceptable operating range.	See Troubleshooting System Cooling Problems.
E1313	Fan Redundancy	The system is no longer fan-redundant. Another fan failure will put the system at risk of over-heating.	Check control panel LCD for additional scrolling messages. See Troubleshooting System Cooling Problems.
E1410	CPU # IERR	Specified microprocessor is reporting a system error.	See your system's *Information Update Tech Sheet* located on **support.dell.com** for the most current system information. If the problem persists, see Getting Help.
E1414	CPU # Thermtrip	Specified microprocessor is out of acceptable temperature range and has halted operation.	See Troubleshooting System Cooling Problems. If the problem persists, ensure that the microprocessor heat sinks are properly installed. See Troubleshooting the Microprocessors. NOTE: The LCD continues to display this message until the system's power cord is disconnected and reconnected to the AC power source, or the SEL is cleared using either Server Assistant or the BMC Management Utility. See the *Dell OpenManage Baseboard Management Controller User's Guide* for information about these utilities.
E1418	CPU # Presence	Specified processor is missing or bad, and the system is in an unsupported configuration	See Troubleshooting the Microprocessors.
E141C	CPU Mismatch	Processors are in a configuration unsupported by Dell.	Ensure that your processors match and conform to the type described in the

Code	Text	Causes	Corrective Actions
			Microprocessor Technical Specifications outlined in your system's *Getting Started Guide*.
E141F	CPU Protocol	The system BIOS has reported a processor protocol error.	See Getting Help.
E1420	CPU Bus PERR	The system BIOS has reported a processor bus parity error.	See Getting Help.
E1421	CPU Init	The system BIOS has reported a processor initialization error.	See Getting Help.
E1422	CPU Machine Chk	The system BIOS has reported a machine check error.	See Getting Help.
E1610	PS # Missing	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	See Troubleshooting Power Supplies.
E1614	PS # Status	No power is available from the specified power supply; specified power supply is improperly installed or faulty.	See Troubleshooting Power Supplies.
E1618	PS # Predictive	Power supply voltage is out of acceptable range; specified power supply is improperly installed or faulty.	See Troubleshooting Power Supplies.
E161C	PS # Input Lost	Power source for specified power supply is unavailable, or out of acceptable range	Check the AC power source for the specified power supply. If problem persists, see Troubleshooting Power Supplies.
E1620	PS # Input Range	Power source for specified power supply is unavailable, or out of acceptable range	Check the AC power source for the specified power supply. If problem persists, see Troubleshooting Power Supplies.
E1624	PS Redundancy	The power supply subsystem is no longer redundant. If the last supply fails, the system will go down.	See Troubleshooting Power Supplies.
E1710	I/O Channel Chk	The system BIOS has reported an I/O channel check error.	See Getting Help.
E1711	PCI PERR B## D## F## PCI PERR Slot #	The system BIOS has reported a PCI parity error on a component that resides in PCI configuration space at bus ##, device ##, function ##. The system BIOS has reported a PCI parity error on a component that resides in PCI slot #.	Remove and reseat the PCI expansion cards. If the problem persists, see Troubleshooting Expansion Cards. If the problem persists, the system board is faulty. See Getting Help.

Code	Text	Causes	Corrective Actions
E1712	PCI SERR B## D## F## PCI SERR Slot #	The system BIOS has reported a PCI system error on a component that resides in PCI configuration space at buss ##, device ##, function ##. The system BIOS has reported a PCI system error on a component that resides in slot #.	Remove and reseat the PCI expansion cards. If the problem persists, see Troubleshooting Expansion Cards. If the problem persists, the system board is faulty. See Getting Help.
E1714	Unknown Err	The system BIOS has determined that there has been an error in the system, but is unable to determine its origin.	See Getting Help.
E171F	PCIE Fatal Err B## D## F## PCIE Fatal Err Slot #	The system BIOS has reported a PCIe fatal error on a component that resides in PCI configuration space at bus ##, device ##, function ##. The system BIOS has reported a PCIe fatal error on a component that resides in slot #.	Remove and reseat the PCI expansion cards. If the problem persists, see Troubleshooting Expansion Cards. If the problem persists, the system board is faulty. See Getting Help.
E1810	HDD ## Fault	The SAS subsystem has determined that hard drive ## has experienced a fault.	See Troubleshooting a Hard Drive.
E1811	HDD ## Rbld Abrt	The specified hard drive has experienced a rebuild abort.	See Troubleshooting a Hard Drive. If the problem persists, see your RAID documentation.
E1812	HDD ## Removed	The specified hard drive has been removed from the system.	Information only.
E1913	CPU & Firmware Mismatch	The BMC firmware does not support the CPU.	Update to the latest BMC firmware. See the *BMC User's Guide* for more information on setup and use of BMC.
E1A10	PBD Pwr Cable	The power distribution board power cable is unseated, missing, or bad.	Ensure that the power distribution board power cable is seated properly. If the problem persists, replace the power distribution board power cable. See Installing the Power Distribution Board.
E1A14	SAS Cable A	SAS cable A is unseated, missing, or bad.	Check the cable connection to the SAS backplane. See Cabling the SAS Backplane Boards.
E1A15	SAS Cable B	SAS cable B is unseated, missing, or bad.	Check the cable connection to the SAS backplane. See Cabling the SAS Backplane Boards.

Code	Text	Causes	Corrective Actions
E1A16	SAS Cable FB	Flex bay SAS cable is unseated, missing, or bad.	Check the cable connection to the SAS backplane. See Cabling the SAS Backplane Boards.
E1A17	Pwr Cable FB	Flex bay power cable is unseated, missing, or bad.	Check the power cable connection to the flex bay backplane. See Installing the 1x2 Flex Bay Drive Bracket.
E1A18	PDB Ctrl Cable	The power distribution board control cable is unseated, missing, or bad.	Ensure that the power distribution board control cable is seated properly. If the problem persists, replace the power distribution board control cable. See Installing the Power Distribution Board.
E2010	No Memory	No memory is installed in the system.	Install memory. See Memory.
E2011	Mem Config Err	Memory detected, but is not configurable. Error detected during memory configuration.	See Troubleshooting System Memory.
E2012	Unusable Memory	Memory is configured, but not usable. Memory subsystem failure.	See Troubleshooting System Memory.
E2013	Shadow BIOS Fail	The system BIOS failed to copy its flash image into memory.	See Troubleshooting System Memory.
E2014	CMOS Fail	CMOS failure. CMOS RAM not functioning properly.	See Getting Help.
E2015	DMA Controller	DMA controller failure.	See Getting Help.
E2016	Int Controller	Interrupt controller failure.	See Getting Help.
E2017	Timer Fail	Timer refresh failure.	See Getting Help.
E2018	Prog Timer	Programmable interval timer error	See Getting Help.
E2019	Parity Error	Parity error.	See Getting Help.
E201A	SIO Err	SIO failure.	See Getting Help.
E201B	Kybd Controller	Keyboard controller failure.	See Getting Help.
E201C	SMI Init	System management interrupt (SMI) initialization failure.	See Getting Help.
E201D	Shutdown Test	BIOS shutdown test failure.	See Getting Help.
E201E	POST Mem Test	BIOS POST memory test failure.	See Troubleshooting System Memory. If problem persists, see Getting Help.
E201F	DRAC Config	Dell remote access controller (DRAC) configuration failure.	Check screen for specific error messages.

Code	Text	Causes	Corrective Actions
			Ensure that DRAC cables and connectors are properly seated. If problem persists, see your DRAC documentation.
E2020	CPU Config	CPU configuration failure.	Check screen for specific error messages.
E2021	Memory Population	Incorrect memory configuration. Memory population order incorrect.	Check screen for specific error messages. See Troubleshooting System Memory.
E2022	POST Fail	General failure after video.	Check screen for specific error messages.
E2110	MBE DIMM ## & ##	One of the DIMMs in the set implicated by "## & ##" has had a memory multi-bit error (MBE).	See Troubleshooting System Memory.
E2111	SBE Log Disable DIMM ##	The system BIOS has disabled memory single-bit error (SBE) logging, and will not resume logging further SBEs until the system is rebooted. "##" represents the DIMM implicated by the BIOS.	See Troubleshooting System Memory.
E2112	Mem Spare DIMM ##	The system BIOS has spared the memory because it has determined that the memory had too many errors. "## & ##" represents the DIMM pair implicated by the BIOS.	See Troubleshooting System Memory.
E2113	Mem Mirror DIMM ## & ##	They system BIOS has disabled memory mirroring because it has determined that one half of the mirror has had too many errors. "## & ##" represents the DIMM pair implicated by the BIOS.	See Troubleshooting System Memory.
E2118	Fatal NB Mem CRC	One of the connections in the Fully Buffered DIMM (FBD) memory subsystem link on the Northbound side has failed.	See Troubleshooting System Memory.
E2119	Fatal SB Mem CRC	One of the connections in the FBD memory subsystem link on the Southbound side has failed.	See Troubleshooting System Memory.
I1910	Intrusion	System cover has been removed.	Information only.
I1911	>3 ERRs Chk Log	LCD overflow message. A maximum of three error messages can display sequentially on the LCD. The fourth message displays as the standard overflow message.	Check the SEL for details on the events.

Code	Text	Causes	Corrective Actions
I1912	SEL Full	System Event Log is full of events, and is unable to log any more events.	Clear the log by deleting event entries.
W1228	ROMB Batt < 24hr	Warns predictively that the RAID battery has less than 24 hours of charge left.	Replace RAID battery. See Replacing the SAS RAID Controller Daughter Card Battery.
NOTE: For the full name of an abbreviation or acronym used in this table, see the Glossary.			

Dell Support – Server

All equipment was purchased with Dell Support. The equipment is out of warranty and no extended warranty has been purchased. If support is needed the TFHRC Help Desk is the first point of contact. If Dell needs to be contacted the following information may be useful:

- Model: Dell PowerEdge 2900
- Service Tag:
- Express Code:

The contact information for Dell was www.dell.com/ProSupport Federal Government under support if doing troubleshooting or requesting help. Phone: 1-800-945-3355. A Service Tag will be needed when calling.

Customer Acct: 65207193?

Customer Purchase Order #: DTFH6110F00023?

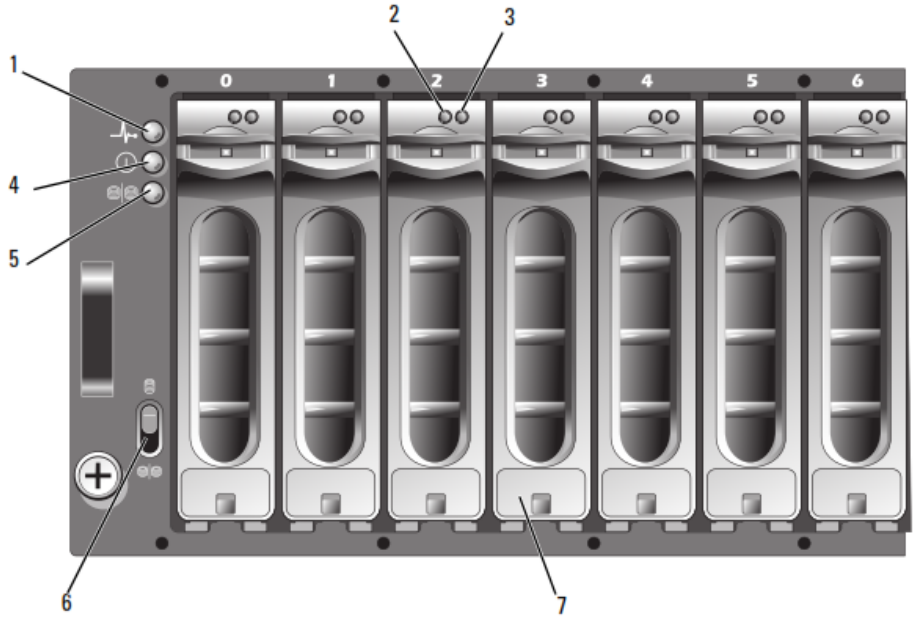
Dell Purchase ID: 2001802580973?

Order Number: 137363466, 137363680 (1 for each unit)?

Storage Status

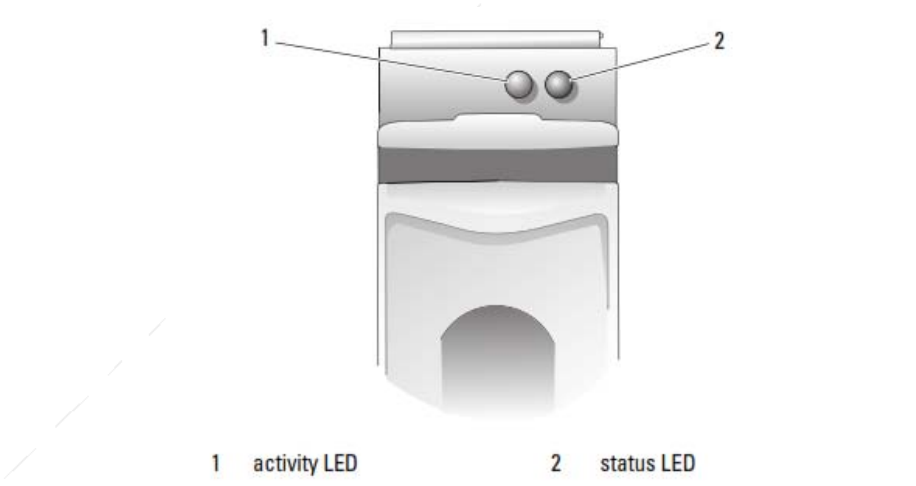
Additional storage was added using two Dell PowerVault MD1000 units with fifteen 2TB SATA hard drives in each. Documentation[13] is stored in …..

[13] http://downloads.dell.com/Manuals/all-products/esuprt_ser_stor_net/esuprt_powervault/powervault-md1000_Owner%27s%20Manual_en-us.pdf, accessed 5/7/2015.



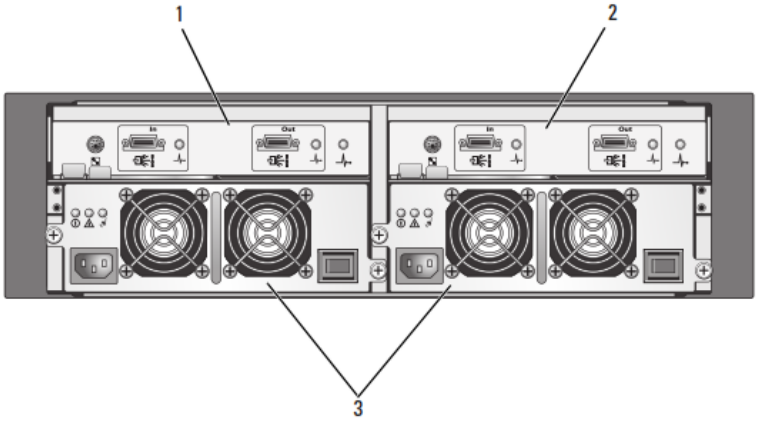
1	enclosure status LED	4	power LED	7	drives (15)
2	drive activity LED	5	split mode LED		
3	drive status LED	6	enclosure mode switch		

Figure 103. Illustration. Front view of Dell PowerVault MD1000.



1 activity LED 2 status LED

Figure 104. Illustration. Hard drive carrier LEDs for MD1000.



1	primary EMM	2	secondary EMM	3	power supply/cooling fan modules (2)

Figure 105. Illustration. Rear of MD1000 unit.

http://downloads.dell.com/Manuals/all-products/esuprt_ser_stor_net/esuprt_powervault/powervault-md1000_Owner%27s%20Manual_en-us.pdf

Dell Support - Storage

All equipment was purchased with Dell Support. The equipment is out of warranty and no extended warranty has been purchased. If support is needed the TFHRC Help Desk is the first point of contact. If Dell needs to be contacted the following information may be useful:

- Model: Dell PowerVault MD100
- Upper unit:
    - Service Tag(located on upper right front of unit outside of enclosure): 8S25XL1:
    - Express Code (located below Service Tag): 1911094765
- Lower unit:
    - Service tag: BR25XL1
    - Express Code: 25580828485

The contact information for Dell was www.dell.com/ProSupport Federal Government under support if doing troubleshooting or requesting help. Phone: 1-800-945-3355. A Service Tag will be needed when calling.

Customer Acct: 65207193

Customer Purchase Order #: DTFH6110F00023

Dell Purchase ID: 2001802580973

Order Number: 137363466, 137363680 (1 for each unit)

Order Number: 137363466, 137363680 (1 for each unit)

Hard Drive Replacement

Hard drive failure is identified by yellow lights in the affected drive bay. New drives are no longer available from Dell nor are refurbished drives. A single replacement drive is on hand for the next drive failure in the server or the attached storage.

Replacement drives can be obtained from xByte Technologeis (http://www.xByte.com). The server and the storage units use 3.5” 2TB SATA hard drives. 7200RPM or slower disk speeds are acceptable. Smaller storage amounts are not. If Dell drives are not available through xByte, compatible replacements may be obtained based on a discussion of drives compatible with the MD1000.[14] The two suitable drives for the LTPP system are:

- Hitachi (Ultrastar A7K2000) SATA 2TB 7.2K RPM (HUA722020ALA330)[15]
- Western Digital (EP500M) SATA 2TB 5.4K RPM (WD2002FYPS-18U1B0)[16]

The drives are effectively plug-and-play. They may be received as bare drives or with carriers. If the drive is received without a carrier, removed the failed drive and swap the drives in the carrier. Replace the drive in the rack. Open the DRAC and start the rebuilding process. It will take several hours to fully restore the system.

UPS

[14] http://www.flagshiptech.com/eBay/Dell/MD1000HDSupportMatrix.pdf, accessed 5/6/2015. Access through http://store.flagship.com and select PowerVault storage, MD 1000.

[15] http://www.newegg.com/Product/Product.aspx?Item=N82E16822145310, accessed 5/6/2015 and identified as Hitachi GST Ultrastar A7K2000 0F10452 2TB 7200 RPM 32MB Cache SATA 3.0Gb/s 3.5" Internal Hard Drive Bare Drive.

[16] http://www.newegg.com/Product/Product.aspx?Item=N82E16822136365, accessed 5/6/2015 and identified as Western Digital WD RE4-GP WD2002FYPS 2TB 64MB Cache SATA 3.0Gb/s 3.5" Hard Drive Bare Drive

The UPS with the Dell 2900 is an APC Smart UPS 2200 (**Error! Reference source not found.**), rack mount which has been discontinued by the manufacturer. It is the lower of the two UPS units in the server rack.

Figure 106. Photos[17]. APC Smart UPS 2200 rack mount UPS front and back DLA model.

The model number is DLA2200RM2U. The serial number is JS0838025983. The unit is out of warranty. In the event of battery failure, a single replacement battery, model RBC43, will be required.

Documentation is stored in…

For routine maintenance look at the front of the UPS to verify that the UPS indicates a full charge and that it is not overloaded. Additionally check the online LED and verify that the light is steady. Any other condition requires checking the troubleshooting section of the user's manual.

The front display panel is shown in figure 107. The line of lights (green) on the left side of the panel indicates the amount of load on the unit. The light of lights (also green) of the right side of the panel indicates the level of battery charge. In the center of the panel are two buttons, a test/power on button on top and the power off button on the bottom. The indicators between the left hand column of lights and the on/off buttons are from top to bottom AVR Trim, Online, and AVR Boost. The indicators between the on/off buttons and the column of lights on the right side are from top to bottom, Overload, On Battery, and Replace Battery/Battery Disconnected.

[17] From http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=DLA2200RM2U&tab=documentation, accessed 5/7/2015

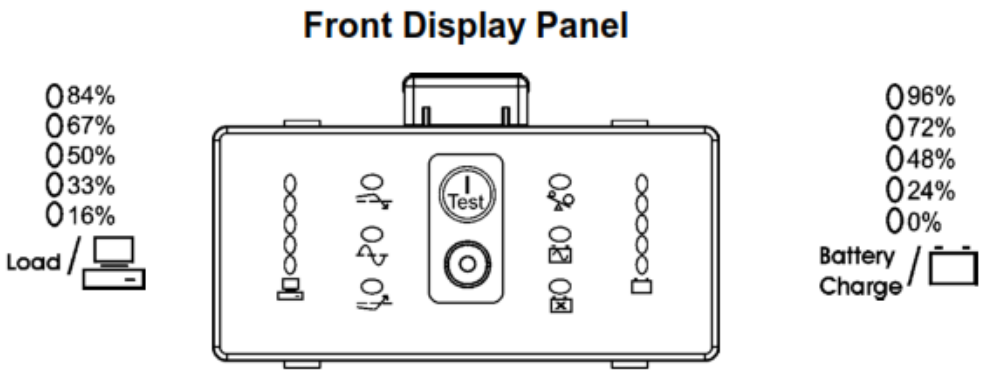


Figure 107. Illustration[18]. DLA 2200 Smart UPS front panel.

AVR trim indicates that the UPS is compensating for high utility voltage. AVR boost in contrast is compensation for low utility voltage. Online means that the UPS is supplying utility power (connected to the outlet) and not using battery power. The indicators between the on/off buttons and the column of lights on the right side are from top to bottom, Overload, On Battery, and Replace Battery/Battery Disconnected. Overload, when lit, indicates that the connected loads are drawing more power than the UPS power rating and requires use of the troubleshooting section of the manual. On battery indicates that utility power is probably off and that shutdown of the attached equipment is recommended. The unit has sufficient power to handle the Dell 2900 and the two MD1000 units for five to fifteen minutes. Replace battery/battery disconnected need to be verified by the user. To check for a user serviceable disconnection, turn the UPS off and remove the front cover of the unit. The battery plugs into the front of the unit and the connection can be unplugged and plugged in. If the battery isn't holding a charge, obtaining a replacement needs to be discussed with the COR. Any more rigorous battery maintenance needs to be handled with the assistance of the TFHRC IT Desk and concurrence of the COR. Additional troubleshooting information is contained in the documentation for the unit.

SOFTWARE

The following is a list of licensed software associated with the Dell 2900. *(Generate a formal list with versioning using Spiceworks.)cover acquisition, update and uses.*

Table 20. Dell 2900 COTS software.

Software	Renewal Date	Renewed by
Symantec Backup Exec 2010 (w/maintenance)	Jan-2014**	FHWA

[18] Illustrations taken from APC User's Guide, http://www.apc.com/products/resource/include/techspec_index.cfm?base_sku=DLA2200RM2U&tab=documentation, accessed 5/7/2015.

Oracle	N/A	DOT*
SQLDeveloper 4.x	Freeware	
MS Office 2007	N/A	DOT
MS Access 2003	N/A	DOT
Winzip		DOT
Adobe Acrobat 9	N/A	DOT
TextPad	Shareware	
Notepad++	Freeware	
PowerDesk 7	Purchase of upgrades only	LTPP
Spiceworks	Freeware	

*Team Leader and COR have licensing information
** Not renewed because operations shifted to new server (10.10.10.34)

Windows Server 2008

This is the operating system for Dell 2900.

Operating system patches are applied through Windows update sporadically with the removal of the server from the internet. The Windows update process was set for manual rather than automatic updates when the computer was connected to the internet. Updates are also applied as requested by the TFHRC Help Desk.

Symantec Anti-Virus

Symantec Endpoint Protection 12.1.5337.5000 is the current version as of May 2015. This is the FHWA provided antivirus program. It requires a manual update while connected to the internet to ensure all elements are current.

The LTPP Administrator does not have administrative rights to change the backup frequencies or folders for this software.

Symantec Backup Exec 2010

Symantec Backup Exec 2010 is being used to perform backups. It requires manual updates to remain current.

Maintenance support ended in February 2014. No updates are being applied. No upgrade will be installed.

Oracle

Oracle was chosen early in the development of the IMS. At the time, it was one of the only tools which could handle large databases across multiple hardware platforms. Oracle also had a forms and reports package for application development which was able to run on multiple platforms without recoding.

The server is on an isolated network with access limited to LTPP personnel. Oracle software updates have generally only been applied during major system upgrades.

The Oracle Database Enterprise Edition version 11.2.0.1.0 along with the administrative tools is installed for use with the PPDB on the Dell 2900. *Add reference on location of documentation locally and on-line.*

SQL Developer

This is Oracle software that provides a Graphical User Interface (GUI) with which to view and manage database objects (tables, views, indices, tablespaces, users, etc.). This software is installed on the server when the Oracle RDBMS is installed. This software replaces the use of Oracle's Enterprise Manager on the Dell 2900.

Limited documentation on the more common uses of this tool for a DBA is found in Appendix M. SQL Developer Notes. Abbreviated documentation is also found in the database engineer's guide on data review and manipulation.

This software is updated when there is a major version change by copying over the new installation package.

SQLPlus Worksheet

The SQLPlus Worksheet is an Oracle client tool that allows the user to type SQL*Plus commands in an input window and see results in an output window. Commands are executed by pressing F5 or CTRL-Enter. Previous commands can be accessed by pressing CTRL-p and next commands by pressing CTRL-n. Other shortcuts are available in this tool. This tool has been replaced by SQL Developer in daily use.

Command Line

SQLPlus and Oracle utilities can be executed from a Command window by users with permissions to access the server directly. For example, a sqlplus file (.sql) can be executed with the following syntax:

```
sqlplus connectstring @sqlfile.sql
```

The Oracle data export command can be executed as follows:

```
exp connectstring parameters.par
```

where the parameters.par file has all input parameters. The same list of parameters can be included on the command line.

PowerDesk7

PowerDesk is file management software similar to Windows Explorer. Its advantage over Windows Explorer is that the results of directory searches may be save to text (.txt) or comma separated value (.csv) files. This product requires a license.

This product has not been updated since installation.

Notepad++

This is a text editor. It is a free source code editor distributed under the GPL license. It is similar to Notepad or Wordpad. Its advantages are that it can do columnar cut and paste, it has basic syntax checking capabilities for SQL and other languages and files can be opened in more than one tool using a text editor and they will be synchronized. The last capability makes it possible edit scripts in Notepad++ and after saving them, run them in SQLDeveloper while having them open in both applications.

This product is updated when a new stable version is available.

Microsoft Office

Office has been installed in order to process data releases efficiently. The tools include Word®, Excel®, Outlook®, Powerpoint® and Access®. Microsoft Office has been installed on this machine primarily to provide Microsoft Access for reviewing tables used by LTPP applications in this format.

This software was updated using Windows Live Update in manual mode. This software is no longer being updated with removal of the Dell 2900 from the internet.

Winzip

Winzip is used for file compression. The original installation on the Dell 2900 was Winzip11. No intermediate upgrades were obtained. In 2014, to maintain compatibility with the DPW, a new version was purchased. As a commercial license, the software may be installed on three machines. The license covers both active servers.

This copy of the software is not being updated.

Spiceworks

This is third party freeware for network management. The software was installed to generate a list of installed applications for IT Security documentation. None of the other functionality is used. It requires access to the internet to function.

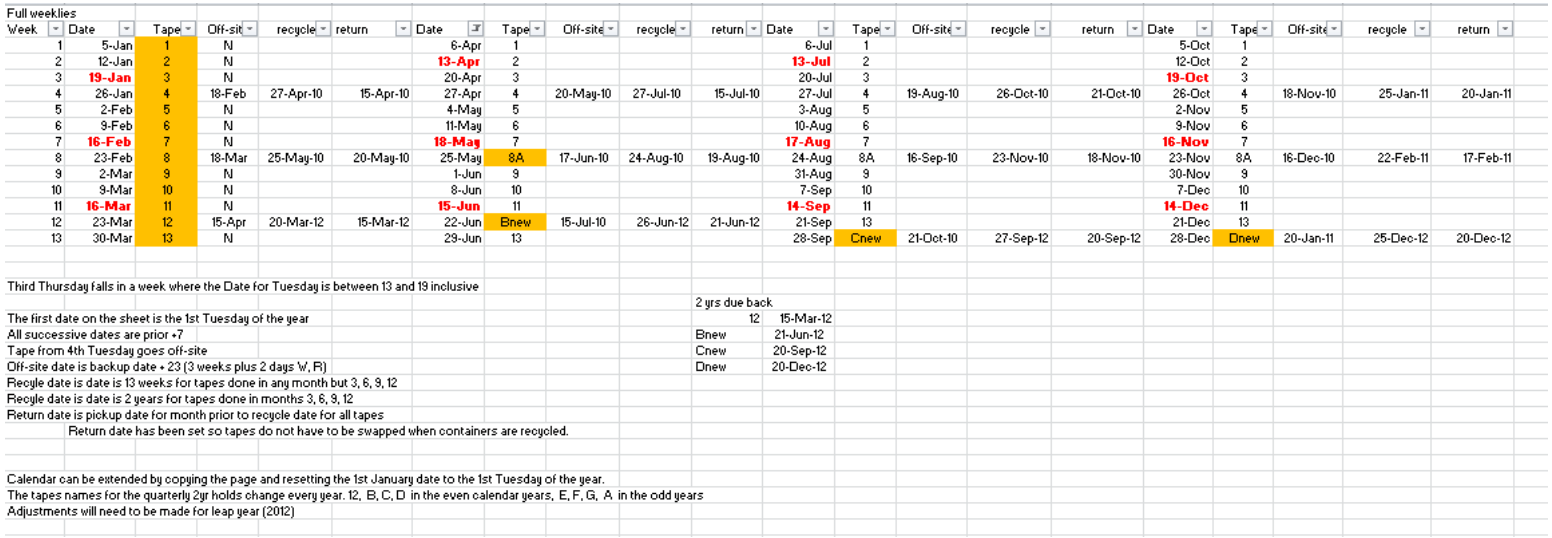
APPENDIX AE. BACKUP POLICIES – DELL 2900

BI-WEEKLY TAPE ROTATION SCHEDULE

The tape rotation for weekly backups is the 13 week schedule discussed in Inputs to Backup Policies. In figure 108 the schedule for 2010 taken from the offsite_rotations spreadsheet is provided. The underlined dates are the weeks that off-site pickup and delivery occurs. The Week column is the number of the week in the quarter. The Date value is the Tuesday backup date. The Tape number is the label on the box and the tape of the tape to be used. When a tape other than the 2-year archive is taken out of the rotation, it is replaced by a tape with the same number and an alpha character. The #8 tape was used to store the 2010 annual submission for indefinite archive. Its replacement is 8A. The off-site column indicates whether or not the tape is sent off-site for storage. It is sent out the following month the indicated Thursday date. The Recycle date is the date that a tape will be reused. It has only been filled in for tapes sent off-site so that the date it needs to be returned from storage can be identified. The recycle date in all cases is the Date value on which the tape is used the next quarter. Tapes identified with an * (asterisk) are on a 2-year archive schedule and the year for recycling is 2012 for the 1st 3 quarters and 2013 for the 4th quarter.

Figure 109 is the 2011 schedule when tape backups shifted from weekly to every other week (bi-weekly). The change was made due to costs associated with media required for both weekly and quarterly backups as the amount of data expanded. The schedule was establish with a rotation cycle of four quarters with the extended retention periods for the last tape of each quarter. *Describe figure 98.*

Figure 110 through figure 112 show the bi-weekly schedules used for 2012 to 2014. In 2015, the Dell 2900 became the backup instead of the primary server and tape backup frequency was reduced to monthly following the SDR and retention of parallel processing capability as shown in figure 113.



Full weeklies

Week	Date	Tape	Off-sit	recycle	return	Date	Tape	Off-site	recycle	return	Date	Tape	Off-site	recycle	return	Date	Tape	Off-site	recycle	return
1	5-Jan	1	N			6-Apr	1				6-Jul	1				5-Oct	1			
2	12-Jan	2	N			**13-Apr**	2				**13-Jul**	2				12-Oct	2			
3	**19-Jan**	3	N			20-Apr	3				20-Jul	3				**19-Oct**	3			
4	26-Jan	4	18-Feb	27-Apr-10	15-Apr-10	27-Apr	4	20-May-10	27-Jul-10	15-Jul-10	27-Jul	4	19-Aug-10	26-Oct-10	21-Oct-10	26-Oct	4	18-Nov-10	25-Jan-11	20-Jan-11
5	2-Feb	5	N			4-May	5				3-Aug	5				2-Nov	5			
6	9-Feb	6	N			11-May	6				10-Aug	6				9-Nov	6			
7	**16-Feb**	7	N			**18-May**	7				**17-Aug**	7				**16-Nov**	7			
8	23-Feb	8	18-Mar	25-May-10	20-May-10	25-May	8A	17-Jun-10	24-Aug-10	19-Aug-10	24-Aug	8A	16-Sep-10	23-Nov-10	18-Nov-10	23-Nov	8A	16-Dec-10	22-Feb-11	17-Feb-11
9	2-Mar	9	N			1-Jun	9				31-Aug	9				30-Nov	9			
10	9-Mar	10	N			8-Jun	10				7-Sep	10				7-Dec	10			
11	**16-Mar**	11	N			**15-Jun**	11				**14-Sep**	11				**14-Dec**	11			
12	23-Mar	12	15-Apr	20-Mar-12	15-Mar-12	22-Jun	Bnew	15-Jul-10	26-Jun-12	21-Jun-12	21-Sep	13				21-Dec	13			
13	30-Mar	13	N			29-Jun	13				28-Sep	Cnew	21-Oct-10	27-Sep-12	20-Sep-12	28-Dec	Dnew	20-Jan-11	25-Dec-12	20-Dec-12

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive

2 yrs due back

12	15-Mar-12
Bnew	21-Jun-12
Cnew	20-Sep-12
Dnew	20-Dec-12

The first date on the sheet is the 1st Tuesday of the year
All successive dates are prior +7
Tape from 4th Tuesday goes off-site
Off-site date is backup date + 23 (3 weeks plus 2 days W, R)
Recyle date is date is 13 weeks for tapes done in any month but 3, 6, 9, 12
Recyle date is date is 2 years for tapes done in months 3, 6, 9, 12
Return date is pickup date for month prior to recycle date for all tapes
Return date has been set so tapes do not have to be swapped when containers are recycled.

Calendar can be extended by copying the page and resetting the 1st January date to the 1st Tuesday of the year.
The tapes names for the quarterly 2yr holds change every year. 12, B, C, D in the even calendar years, E, F, G, A in the odd years
Adjustments will need to be made for leap year (2012)

Figure 108. Screenshot. Weekly tape rotation for 2010.

Bi-Weekly Full Backups

Q1

Week	Date	Tape	Off-site	recycle	return
1	4-Jan	1	N		
2	11-Jan	2	N		
3	18-Jan	3	N		
4	25-Jan	4	17-Feb	26-Apr-11	21-Apr-11
5	1-Feb	5	N		
6	8-Feb	6	N		
7	15-Feb	7	N		
8	22-Feb	8A	17-Mar	24-May-11	19-May-11
9	1-Mar	9	N		
10	8-Mar	10	N		
11	15-Mar	11	N		
12	22-Mar	E	21-Apr	26-Mar-13	21-Mar-13
13	29-Mar	13	N		

Q2

	5-Apr	1	21-Apr	12-Jul-11	16-Jun-11
	12-Apr				
	19-Apr	2		26-Jul-11	
	26-Apr				
	3-May	3	19-May	9-Aug-11	21-Jul-11
	10-May				
	17-May	4		23-Aug-11	
	24-May				
	31-May	5	16-Jun	6-Sep-11	18-Aug-11
	7-Jun				
	14-Jun	6		20-Sep-11	
	21-Jun				
	28-Jun	7	21-Jul	25-Jun-13	20-Jun-13

Q3

Backup Date	Tape	Off-site	Recycle	Return
5-Jul				
12-Jul	1		4-Oct-11	
19-Jul				
26-Jul	2	18-Aug	18-Oct-11	15-Sep-11
2-Aug				
9-Aug	3		1-Nov-11	
16-Aug				
23-Aug	4	15-Sep	15-Nov-11	20-Oct-11
30-Aug				
6-Sep	5		29-Nov-11	
13-Sep				
20-Sep	6		13-Dec-11	
27-Sep				

Q4

4-Oct	1	20-Oct	10-Jan-12	15-Dec-11
11-Oct				
18-Oct	2		24-Jan-12	
25-Oct				
1-Nov	3	17-Nov	7-Feb-12	19-Jan-12
8-Nov				
15-Nov	4		21-Feb-12	
22-Nov				
29-Nov	5	15-Dec	6-Mar-12	16-Feb-12
6-Dec				
13-Dec	6		20-Mar-12	
20-Dec				
27-Dec	8A	19-Jan	24-Dec-13	19-Dec-13

2YR HOLI	out	due back	next use
12	15-Apr-10	15-Mar-12	spare
B	15-Jul-10	21-Jun-12	spare
C	21-Oct-10	20-Sep-12	spare
D	20-Jan-11	20-Dec-12	spare
E	21-Apr-11	21-Mar-13	spare
7	21-Jul-11	20-Jun-13	25-Jun-13
8A	19-Jan-12	19-Dec-13	24-Dec-13

box A	CS01
box B	CS02
box C	CS03
his	

1. Full bi-weekly backups scheduled for every other Tuesday
2. Quarterly rotation schedule
3. Off-site backup pickup scheduled for third Thursday of each month
4. Most recent backup-1 is sent off-site
5. Recycle date is next date that tape is needed (Date + 14*7)
6. Return date is the pickup date before the recycle date
7. Last bi-weekly off-site backup of the 2nd and 4th quarters are kept off-site for 2 years

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive (week with date in red)
Underlined dates are linked to other sheets in book

Figure 109. Screenshot. Bi-weekly tape rotation 2011.

Bi-Weekly Full Backups

Q1

Week	Date	Tape	Off-site	recycle	return
1	3-Jan				
2	10-Jan	1		3-Apr-12	
3	17-Jan				
4	24-Jan	2	16-Feb	17-Apr-12	15-Mar-12
5	31-Jan				
6	7-Feb	3		1-May-12	
7	14-Feb				
8	21-Feb	4	15-Mar	15-May-12	19-Apr-12
9	28-Feb				
10	6-Mar	5		29-May-12	
11	13-Mar				
12	20-Mar	6		12-Jun-12	
13	27-Mar				

Q2

	3-Apr	1	19-Apr	10-Jul-12	21-Jun-12
	10-Apr				
	17-Apr	2		24-Jul-12	
	24-Apr				
	1-May	3	17-May	7-Aug-12	19-Jul-12
	8-May				
	15-May	4		21-Aug-12	
	22-May				
	29-May	5	21-Jun	4-Sep-12	16-Aug-12
	5-Jun				
	12-Jun	6		18-Sep-12	
	19-Jun				
	26-Jun	9	19-Jul	17-Jun-14	15-May-14

Q3

Backup Date	Tape	Off-site	Recycle	Return
3-Jul				
10-Jul	1		2-Oct-12	
17-Jul				
24-Jul	2	16-Aug	16-Oct-12	20-Sep-12
31-Jul				
7-Aug	3		30-Oct-12	
14-Aug				
21-Aug	4		13-Nov-12	
28-Aug				
4-Sep	5	20-Sep	27-Nov-12	15-Nov-12
11-Sep				
18-Sep	6		11-Dec-12	15-Nov-12
25-Sep				

Q4

2-Oct	1	18-Oct	8-Jan-13	20-Dec-12
9-Oct				
16-Oct	2		22-Jan-13	
23-Oct				
30-Oct	3	15-Nov	5-Feb-13	17-Jan-13
6-Nov				
13-Nov	4		19-Feb-13	
20-Nov				
27-Nov	5	20-Dec	5-Mar-13	21-Feb-13
4-Dec				
11-Dec	6		19-Mar-13	
18-Dec				
25-Dec	10	17-Jan	30-Dec-14	18-Dec-14

box A				
box B	CS02	2yr rotation?		
box C				
his				

from	2YR HOLI	out	due back	next use
2010	12	15-Apr-10	15-Mar-12	spare
2010	B	15-Jul-10	21-Jun-12	spare
2010	C	21-Oct-10	20-Sep-12	spare
2010	D	20-Jan-11	20-Dec-12	spare
2011	E	21-Apr-11	21-Mar-13	spare
2011	7	21-Jul-11	20-Jun-13	25-Jun-13
2011	8A	19-Jan-12	19-Dec-13	24-Dec-13
2012	9	19-Jul-12	15-May-14	17-Jun-14
2012	10	17-Jan-13	18-Dec-14	30-Dec-14

1. Full bi-weekly backups scheduled for every other Tuesday
2. Quarterly rotation schedule
3. Off-site backup pickup scheduled for third Thursday of each month
4. Most recent backup-1 is sent off-site
5. Recycle date is next date that tape is needed (Date + 14*7)
6. Return date is the pickup date before the recycle date
7. Last bi-weekly off-site backup of the 2nd and 4th quarters are kept off-site for 2 years

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive (week with date in red)
Underlined dates are linked to other sheets in book

Figure 110. Screenshot. Bi-weekly tape rotation 2012.

Bi-Weekly Full Backups

Q1

Week	Date	Tape	Off-site	recycle	return
1	1-Jan				
2	8-Jan	1		2-Apr-13	
3	15-Jan				
4	22-Jan	2		16-Apr-13	
5	29-Jan				
6	5-Feb	3	21-Feb	30-Apr-13	18-Apr-13
7	12-Feb				
8	19-Feb	4		14-May-13	
9	26-Feb				
10	5-Mar	5	21-Mar	28-May-13	16-May-13
11	12-Mar				
12	19-Mar	6		11-Jun-13	
13	26-Mar				

Q2

	2-Apr	1	18-Apr	9-Jul-13	20-Jun-13
	9-Apr				
	16-Apr	2		23-Jul-13	
	23-Apr				
	30-Apr	3	16-May	6-Aug-13	18-Jul-13
	7-May				
	14-May	4		20-Aug-13	
	21-May				
	28-May	5	20-Jun	3-Sep-13	15-Aug-13
	4-Jun				
	11-Jun	6		17-Sep-13	
	18-Jun				
	25-Jun	7	18-Jul	30-Jun-15	18-Jun-15

Q3

Backup Date	Tape	Off-site	Recycle	Return
2-Jul				
9-Jul	1		1-Oct-13	
16-Jul				
23-Jul	2	15-Aug	15-Oct-13	19-Sep-13
30-Jul				
6-Aug	3		29-Oct-13	
13-Aug				
20-Aug	4		12-Nov-13	
27-Aug				
3-Sep	5	19-Sep	26-Nov-13	21-Nov-13
10-Sep				
17-Sep	6		10-Dec-13	
24-Sep				

Q4

1-Oct	1	17-Oct	7-Jan-14	19-Dec-13
8-Oct				
15-Oct	2		21-Jan-14	
22-Oct				
29-Oct	3	21-Nov	4-Feb-14	16-Jan-14
5-Nov				
12-Nov	4		18-Feb-14	
19-Nov				
26-Nov	5	19-Dec	4-Mar-14	20-Feb-14
3-Dec				
10-Dec	6		18-Mar-14	
17-Dec				
24-Dec	11	16-Jan	29-Dec-15	17-Dec-15
31-Dec				

box A
box B
box C
his

from	2YR HOLI	out	due back	next use
2010	12	15-Apr-10	15-Mar-12	24-Jun-14
2010	B	15-Jul-10	21-Jun-12	spare
2010	C	21-Oct-10	20-Sep-12	spare
2010	D	20-Jan-11	20-Dec-12	spare
2011	E	21-Apr-11	21-Mar-13	spare
2011	7	21-Jul-11	20-Jun-13	25-Jun-13
2011	8A	19-Jan-12		
2012	9	19-Jul-12	17-Jul-14	
2012	10	17-Jan-13	30-Dec-14	
2013	7	18-Jul-13	18-Jun-15	30-Jun-15
2013	11	16-Jan-14	17-Dec-15	29-Dec-15

1. Full bi-weekly backups scheduled for every other Tuesday
2. Quarterly rotation schedule
3. Off-site backup pickup scheduled for third Thursday of each month
4. Most recent backup-1 is sent off-site
5. Recycle date is next date that tape is needed (Date + 14*7)
6. Return date is the pickup date before the recycle date
7. Last bi-weekly off-site backup of the 2nd and 4th quarters are kept off-site for 2 years

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive (week with date in red)
Underlined dates are linked to other sheets in book

Figure 111. Screenshot. Bi-weekly tape rotation 2013.

Bi-Weekly Full Backups

Q1

Week	Date	Tape	Off-site	recycle	return
1	7-Jan	1		8-Apr-14	
2	14-Jan				
3	21-Jan	2		22-Apr-14	
4	28-Jan				
5	4-Feb	3	20-Feb	6-May-14	17-Apr-14
6	11-Feb				
7	18-Feb	4		20-May-14	
8	25-Feb				
9	4-Mar	5	20-Mar	3-Jun-14	15-May-14
10	11-Mar				
11	18-Mar	6		17-Jun-14	
12	25-Mar				
13					

Q2

	1-Apr	1	17-Apr	1-Jul-14	19-Jun-14
	8-Apr				
	15-Apr	2		15-Jul-14	
	22-Apr				
	29-Apr	3	15-May	29-Jul-14	17-Jul-14
	6-May				
	13-May	4		12-Aug-14	
	20-May				
	27-May	5	19-Jun	26-Aug-14	21-Aug-14
	3-Jun				
	10-Jun	6		9-Sep-14	
	17-Jun				
	24-Jun	12	17-Jul	2016	#N/A

Q3

Backup Date	Tape	Off-site	Recycle	Return
1-Jul				
8-Jul	1		7-Oct-14	
15-Jul				
22-Jul	2		21-Oct-14	
29-Jul				
5-Aug	3	21-Aug	4-Nov-14	16-Oct-14
12-Aug				
19-Aug	4		18-Nov-14	
26-Aug				
2-Sep	5	18-Sep	2-Dec-14	20-Nov-14
9-Sep				
16-Sep	6		16-Dec-14	
23-Sep				
30-Sep	spare	16-Oct	30-Dec-14	18-Dec-14

Q4

7-Oct	1		13-Jan-15		
14-Oct					
21-Oct	2		27-Jan-15		
28-Oct					
4-Nov	3	20-Nov	10-Feb-15	15-Jan-15	
11-Nov					
18-Nov	4		24-Feb-15		
25-Nov					
2-Dec	5	18-Dec	10-Mar-15	19-Feb-15	
9-Dec					
16-Dec	6		24-Mar-15		
23-Dec					
30-Dec	13	15-Jan	2016	#N/A	

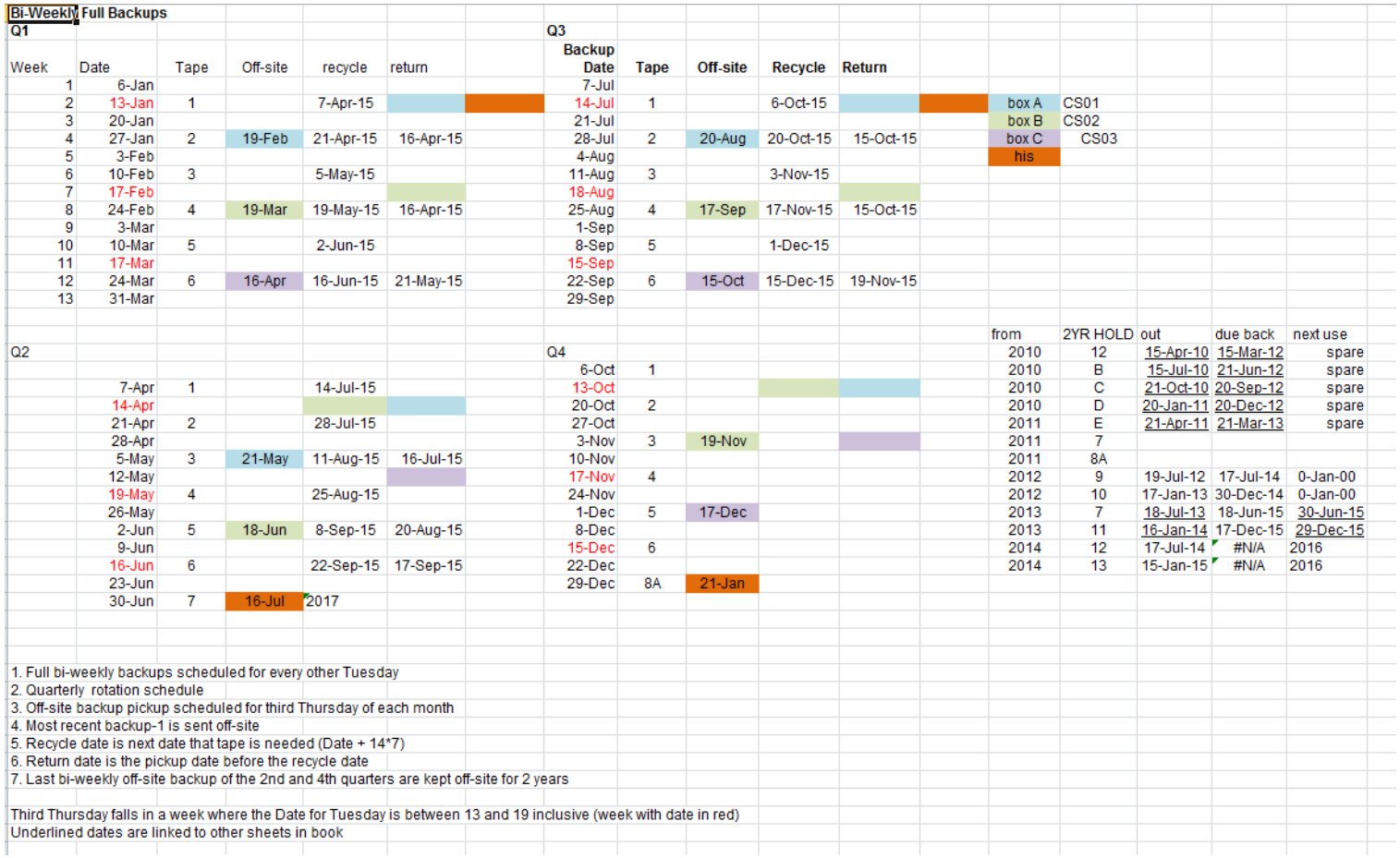
box A
box B
box C
his

from	2YR HOLD	out	due back	next use
2010	12	15-Apr-10	15-Mar-12	24-Jun-14
2010	B	15-Jul-10	21-Jun-12	spare
2010	C	21-Oct-10	20-Sep-12	spare
2010	D	20-Jan-11	20-Dec-12	spare
2011	E	21-Apr-11	21-Mar-13	spare
2011	7			
2011	8A			
2012	9	19-Jul-12	17-Jul-14	
2012	10	17-Jan-13	30-Dec-14	
2013	7	18-Jul-13	18-Jun-15	30-Jun-15
2013	11	16-Jan-14	17-Dec-15	29-Dec-15
2014	12	17-Jul-14	#N/A	2016
2014	13	15-Jan-15	#N/A	2016

1. Full bi-weekly backups scheduled for every other Tuesday
2. Quarterly rotation schedule
3. Off-site backup pickup scheduled for third Thursday of each month
4. Most recent backup-1 is sent off-site
5. Recycle date is next date that tape is needed (Date + 14*7)
6. Return date is the pickup date before the recycle date
7. Last bi-weekly off-site backup of the 2nd and 4th quarters are kept off-site for 2 years

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive (week with date in red)
Underlined dates are linked to other sheets in book

Figure 112. Screenshot. Bi-weekly tape rotation 2014.



Bi-Weekly Full Backups

Q1

Week	Date	Tape	Off-site	recycle	return
1	6-Jan				
2	13-Jan	1		7-Apr-15	
3	20-Jan				
4	27-Jan	2	19-Feb	21-Apr-15	16-Apr-15
5	3-Feb				
6	10-Feb	3		5-May-15	
7	17-Feb				
8	24-Feb	4	19-Mar	19-May-15	16-Apr-15
9	3-Mar				
10	10-Mar	5		2-Jun-15	
11	17-Mar				
12	24-Mar	6	16-Apr	16-Jun-15	21-May-15
13	31-Mar				

Q2

	7-Apr	1		14-Jul-15	
	14-Apr				
	21-Apr	2		28-Jul-15	
	28-Apr				
	5-May	3	21-May	11-Aug-15	16-Jul-15
	12-May				
	19-May	4		25-Aug-15	
	26-May				
	2-Jun	5	18-Jun	8-Sep-15	20-Aug-15
	9-Jun				
	16-Jun	6		22-Sep-15	17-Sep-15
	23-Jun				
	30-Jun	7	16-Jul	2017	

Q3

Backup Date	Tape	Off-site	Recycle	Return
7-Jul				
14-Jul	1		6-Oct-15	
21-Jul				
28-Jul	2	20-Aug	20-Oct-15	15-Oct-15
4-Aug				
11-Aug	3		3-Nov-15	
18-Aug				
25-Aug	4	17-Sep	17-Nov-15	15-Oct-15
1-Sep				
8-Sep	5		1-Dec-15	
15-Sep				
22-Sep	6	15-Oct	15-Dec-15	19-Nov-15
29-Sep				

Q4

6-Oct	1			
13-Oct				
20-Oct	2			
27-Oct				
3-Nov	3	19-Nov		
10-Nov				
17-Nov	4			
24-Nov				
1-Dec	5	17-Dec		
8-Dec				
15-Dec	6			
22-Dec				
29-Dec	8A	21-Jan		

box A	CS01			
box B	CS02			
box C	CS03			
his				

from	2YR HOLD	out	due back	next use
2010	12	15-Apr-10	15-Mar-12	spare
2010	B	15-Jul-10	21-Jun-12	spare
2010	C	21-Oct-10	20-Sep-12	spare
2010	D	20-Jan-11	20-Dec-12	spare
2011	E	21-Apr-11	21-Mar-13	spare
2011	7			
2011	8A			
2012	9	19-Jul-12	17-Jul-14	0-Jan-00
2012	10	17-Jan-13	30-Dec-14	0-Jan-00
2013	7	18-Jul-13	18-Jun-15	30-Jun-15
2013	11	16-Jan-14	17-Dec-15	29-Dec-15
2014	12	17-Jul-14	#N/A	2016
2014	13	15-Jan-15	#N/A	2016

1. Full bi-weekly backups scheduled for every other Tuesday
2. Quarterly rotation schedule
3. Off-site backup pickup scheduled for third Thursday of each month
4. Most recent backup-1 is sent off-site
5. Recycle date is next date that tape is needed (Date + 14*7)
6. Return date is the pickup date before the recycle date
7. Last bi-weekly off-site backup of the 2nd and 4th quarters are kept off-site for 2 years

Third Thursday falls in a week where the Date for Tuesday is between 13 and 19 inclusive (week with date in red)
Underlined dates are linked to other sheets in book

Figure 113. Screenshot. Bi-weekly tape rotation 2015.(update)

QUARTERLY TAPE ROTATION SCHEDULE

The quarterly tape rotation schedule includes AIMS and archival backups. These backups are done the first week of February, May, August and November. These backups require at least two 500GB tapes and two days to complete since verification is included in the process. *The folders backed up include ….*

Insert tape rotation calendar here

Figure 114. Screenshot. Quarterly tape rotation schedule.

INPUTS TO BACKUP POLICIES

This material is derived from the FHWA July 2009 backup procedures document. This system does not include indefinite archives. Indefinite archives are covered in the annual data submission and the NARA submission.

The frequency of backup to cartridge by server drive has been established based on drive usage. The inclusion of incremental backups for drives backed up weekly to cartridge was initiated when additional "external" storage was installed.

Table 21. Database server frequencies.

Drive Letter	Partition Name	Total GB	Update Cycle	Backup Frequency
C:	OS	40	Continuous	Weekly
D:	Working Storage	1,710	Continuous	Incremental #1 Weekly
E:	AIMS	1,710	Annual	Last and first quarter of year
F:	Traffic	1,210	N/A	Incremental #3 Quarterly
G:	Database	1,670	Annual for core data (uploads); Continuous for analysis	Incremental #2 Incremental #4 Weekly
H:	Recovery	3	Never. Dell recovery area.	Never
var	USB port		N/A – drives connected for upload of data	
J:	Backup device		N/A – backup cartridges	
K:	Archive	50,000	Topic dependent –; Some materials have external drive backup on a topic specific basis	Quarterly

Using following logic results in the “ideal” 13-week cycle:

- A minimum of 13 weeks exists between reuse of a cartridge
- Every 4th cartridge used is stored off-site for a 13-week period
- Off-site storage occurs 2-weeks after the backup occurs
- A recycled cartridge from off-site is used the week after it returns from storage
- The last backup of a calendar quarter is stored off-site for 2 years before recycling
- A new cartridge is used for each backup stored off-site for 2 years for the 1st two years. This is cartridge #12 for the 1st 2-year backup and A-G for the next 7 in the cycle.

The ideal cycle has been modified because cartridge pickups are a fixed week of the month and not a fixed interval. A spreadsheet, offsite_rotationsNN.xls, saved in G_Task Order 1…\Task_D_IMS_Hardware-Software\1_Database Operation\a_Operating the Database\0_Backup_Procedures was used to develop the annual calendar and container rotation schedules for the various backups. The modification has been designed to avoid, to the extent possible, swapping backup cartridges in and out of storage boxes at the time of pick up.

The 13 week cycle implemented uses the following logic:

A minimum of 13 weeks exists between reuse of a cartridge

The cartridge for the 4th week of every month cartridge used is stored off-site

Cartridges from the 4th week of the 1st and 2nd months in a quarter are stored off-site for a 13-week period

Cartridges 4th week of the 3rd months in a quarter are stored off-site for a 2-year period

Off-site storage occurs the 3rd week of the following month

A new cartridge is used for each backup stored off-site for 2 years for the 1st two years. This is cartridge #12 for the 1st 2-year backup and A-G for the next 7 in the cycle.

The following has been designated the “ideal” quarterly cycle for backups using the following logic:

A minimum of a year exists between reuse of a cartridge

Cartridges from the first three backups in a calendar year are stored off-site for a year

Off-site storage occurs the quarter after the backup occurs

A recycled cartridge from off-site is used the quarter after it returns from storage

The last backup of a calendar year is stored off-site for 2 years before recycling

None of the quarterly backups are retained indefinitely

APPENDIX AF. SYMANTEC BACKUP EXEC 2010

SYMANTEC ADMINISTRATION AND TROUBLESHOOTING

Passwords

Each user of Symantec Backup must be identified to the software by name and password. The users in Symantec have accounts whose names may or may not match those of their server login accounts. The passwords for the user logon accounts much match those of the server.

Symantec User Accounts

For the purposes of backup, the user for logon to the server and the Symantec software is zsymantec_user. If this user name changes several items must be changed in the Symantec software to continue to use the system. One is the ownership of the selection lists.

On the menu bar pick edit/manage selection lists at which the following dialog box comes up.

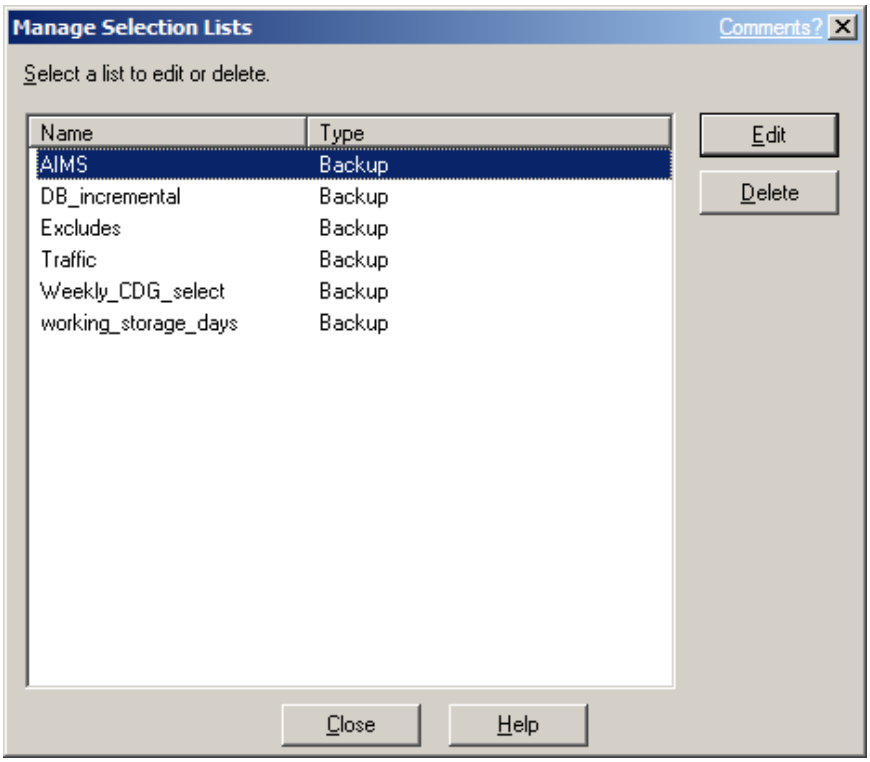


Figure 115. Screenshot. Picking a selection list to create a job.

Each list must be checked via edit for a valid logon account.

When “Edit” is selected the screen in figure 116 will appear.

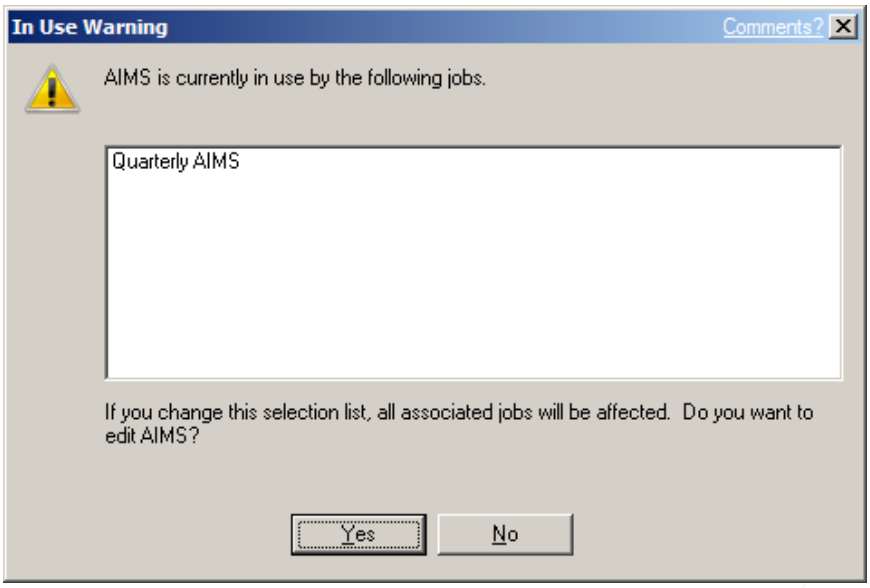


Figure 116. Screenshot. Confirming changes to a selection list with impacts identified.

Click on “Yes” and then on the screen shown in Figure 117 click on ‘Resource Credentials’ in the left most column under Source.

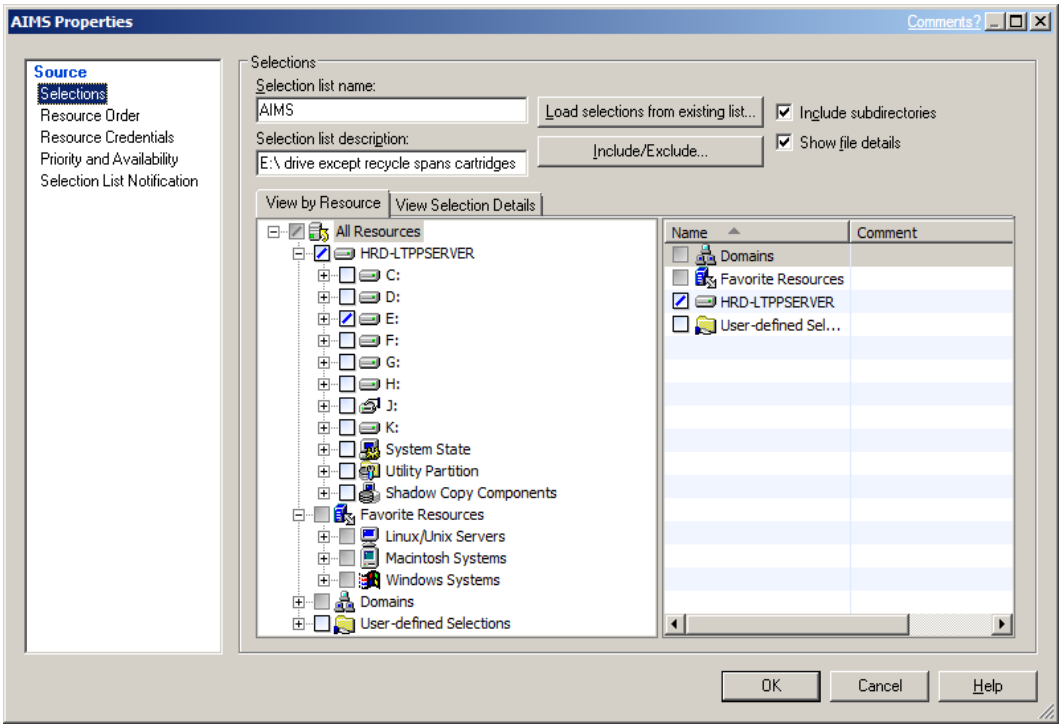


Figure 117. Screenshot. Making folder and file selections for backup.

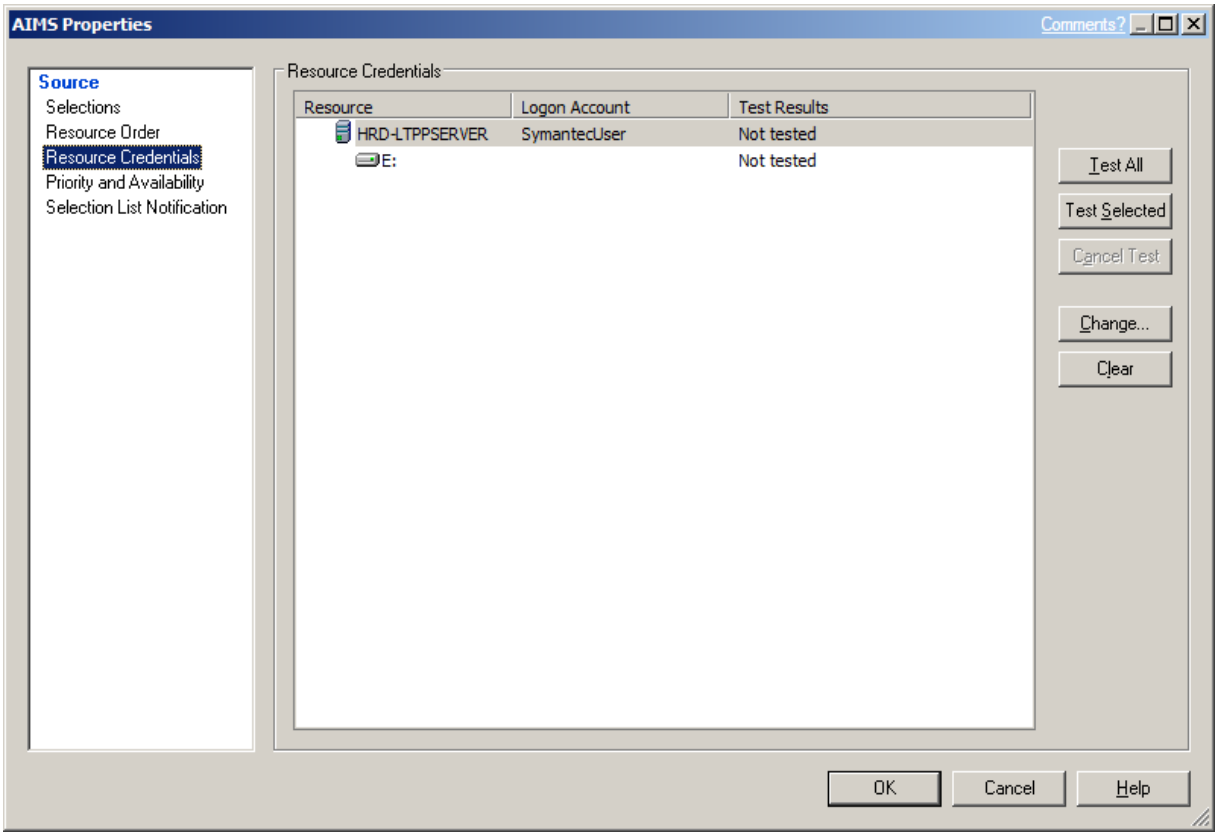


Figure 118. Screenshot. Verifying access to drives identified in backup selections.

If the logon account does not exist on the server it must be changed using Change.

Change will bring up a list of users. Select the appropriate user and click ok.

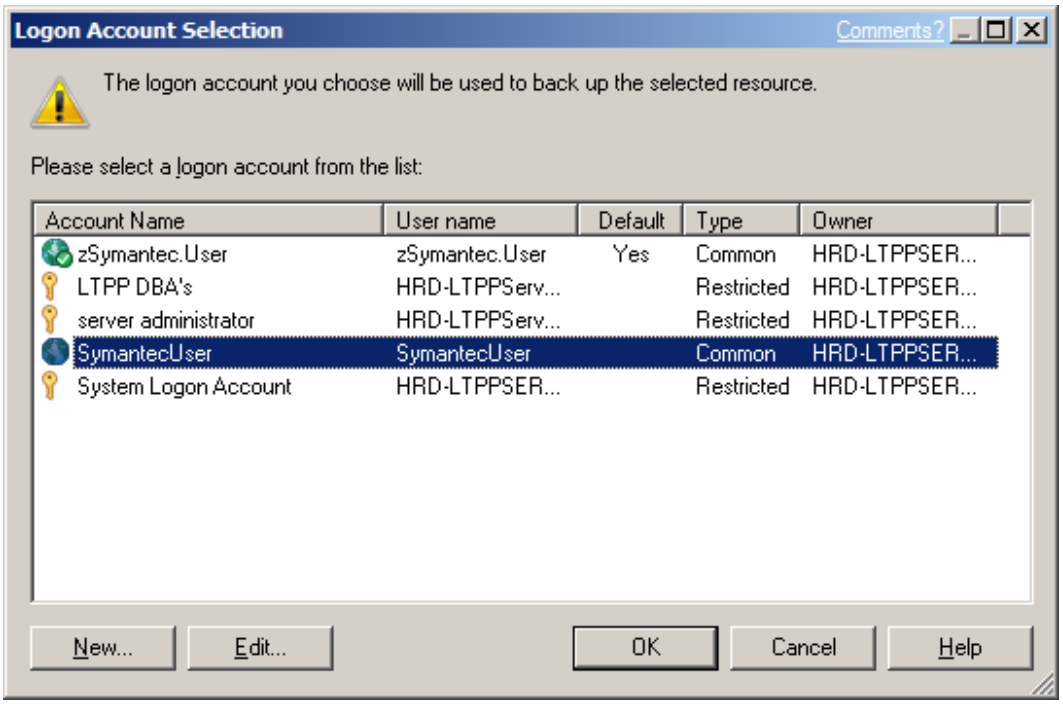


Figure 119. Screenshot. Picking a Logon Account to Run a Backup Job

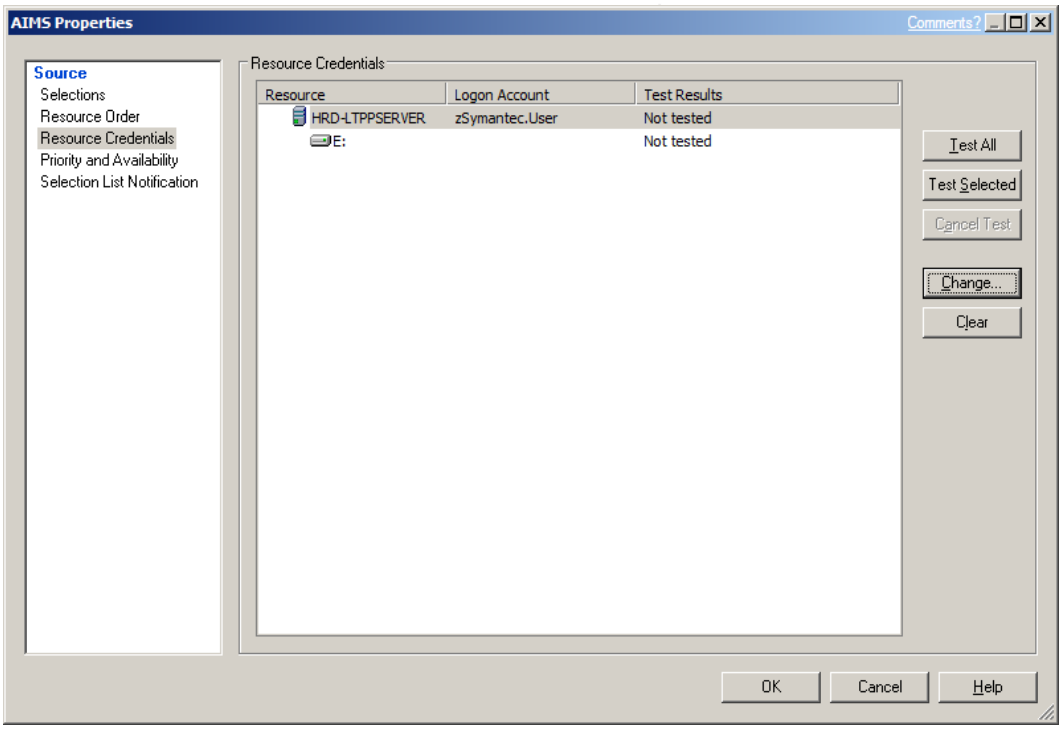


Figure 120. Screenshot. Preparing to Test Access for Backups

Test the Selected or All depending on the number of accounts.

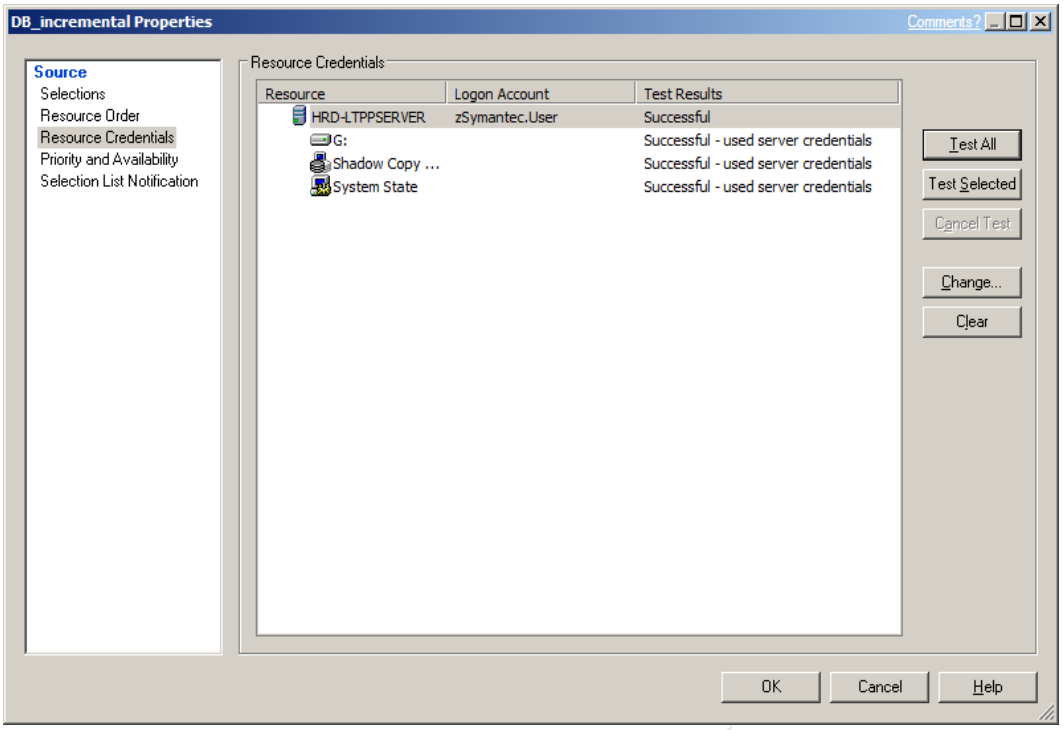


Figure 121. Screenshot. Successful Access Test

A successful test should be accepted by clicking on OK. If it is not successful troubleshoot based on error message displayed.

APPENDIX AG. SYMANTEC 2010 – DOING BACKUPS

CREATING A JOB

A job is created from the Job Setup screen shown in Figure 122. Either the New Job or New job using wizard option from the Backup Tasks box on the left hand side of the screen can be used.

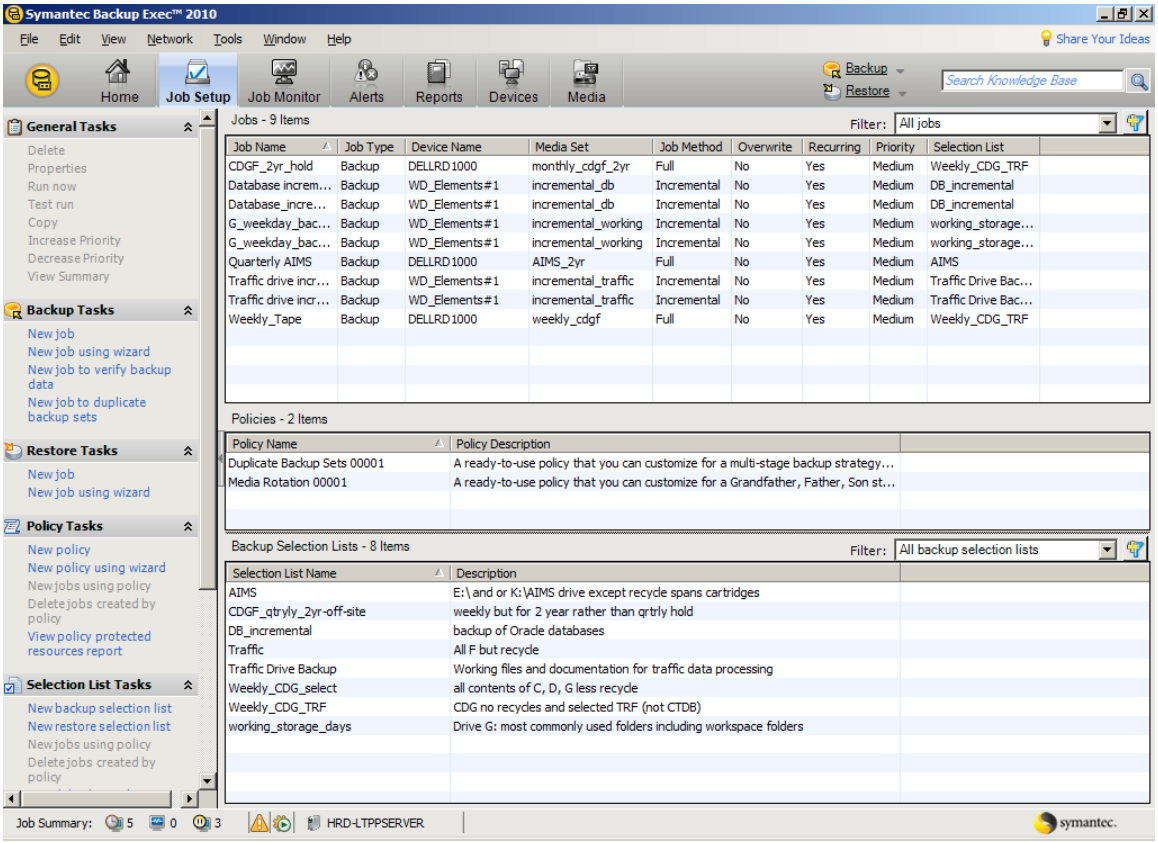


Figure 122. Screenshot. Symantec BE job set up screen.

The upper left box, General Tasks, on the screen has several functions that may be useful: Delete, Properties, Run now, and Test run. Copy is a between server function and not applicable to the LTPP system. These are discussed in Managing jobs.

This discussion goes through the process using the New job option.

Start by clicking on New Job. This will bring up figure 123. The first activity is to select the items to be backed up. If this is the first time this collection of folders/files has been backed up, enter a descriptive name for the list of items under Selection list name to replace the Backup NNNNN naming. Below the name write some text about the materials in the backup.

Do not select show file details unless a by directory listing is absolutely necessary. The list generated in the expanded job log will run to hundreds of pages.

Select the folders and files from each drive.

4. The right hand selection block starting with Domains is not applicable for LTPP.

5. It is recommended to save time and space that the recycle bin not be backed.

6. System state and Shadow Copy Components should generally be included.

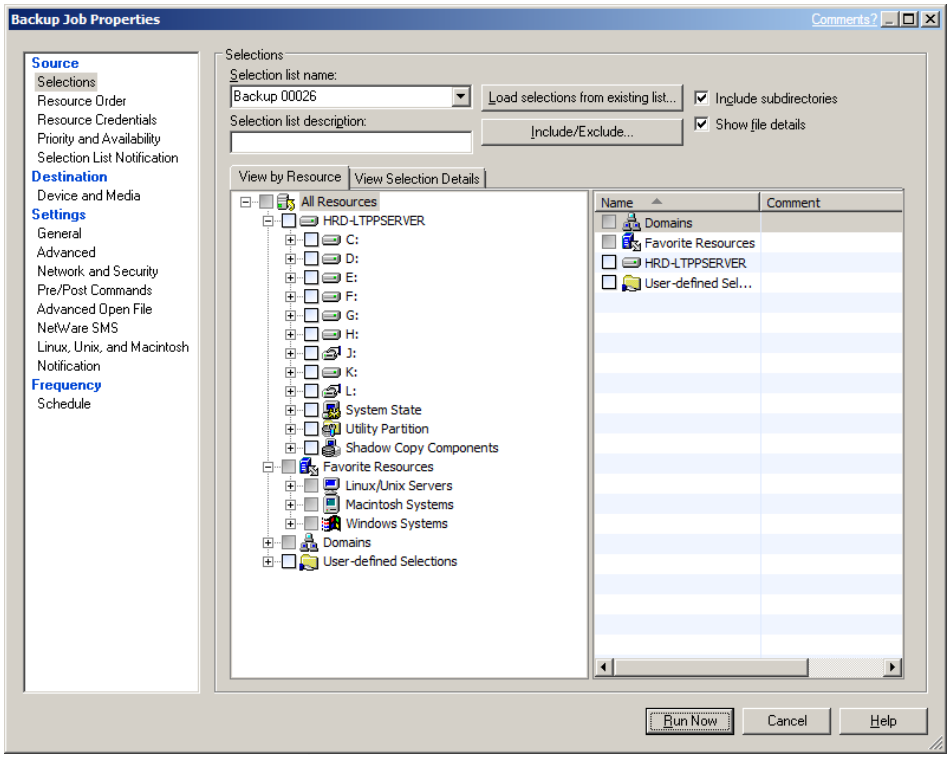


Figure 123. Screenshot. Starting a new job – Selections.

If this is a copy or variant of an existing backup (incremental version of a full backup for example), click on the arrow beside Backup NNNNN to get a list of existing selection lists (figure 123.) Clicking on the preferred list will populate all the selections as shown in figure 30. The right slash indicates only some of the items are being included. A check mark indicates all items are being included.

If the selection list is going to be a combination of new items and existing lists use the Load selections from existing list option. This will bring up figure 31 or an equivalent list to pick from.

The Include/Exclude option is not currently being used. If the server were having files permanently deleted, or only a specific period was desired in a backup or a differential backup was desired those capabilities can be executed through this selection option.

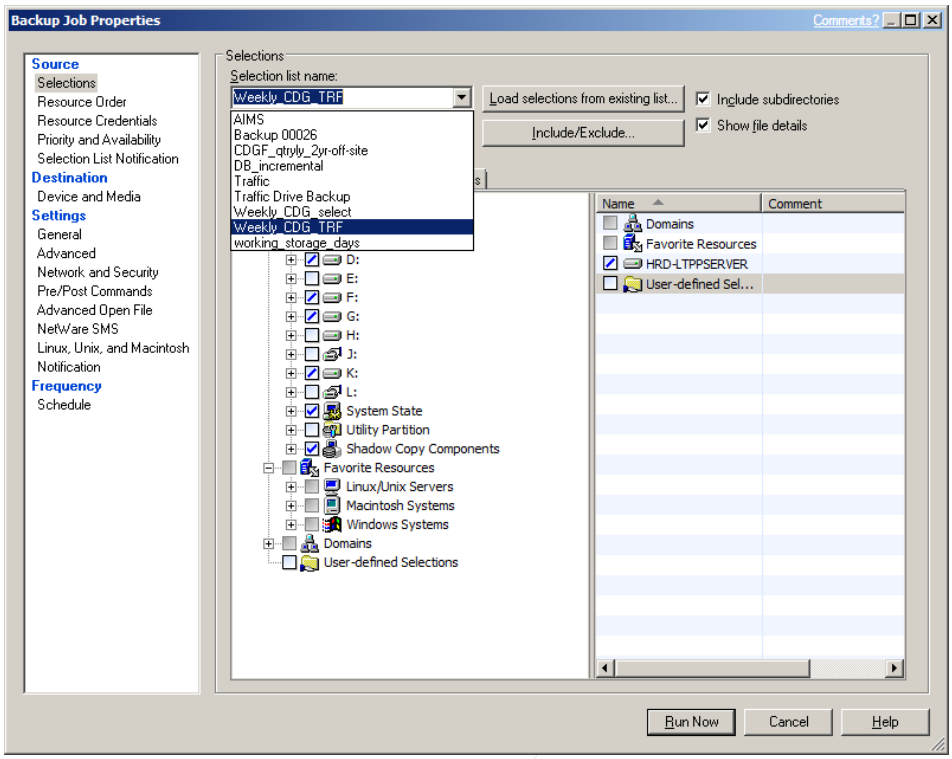


Figure 124. Screenshot. Picking from existing selection lists.

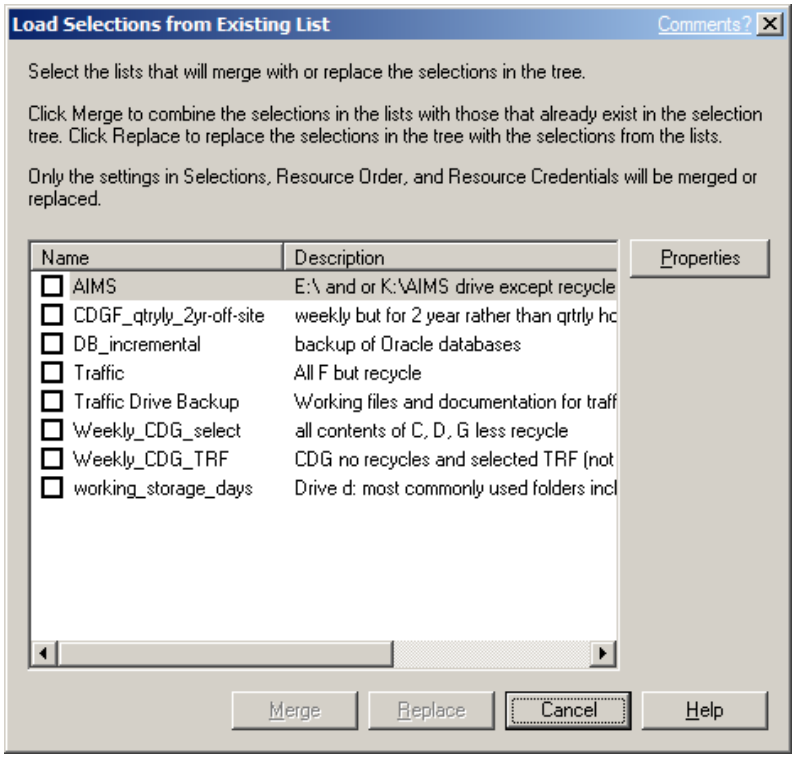


Figure 125. Screenshot. Merge selection options

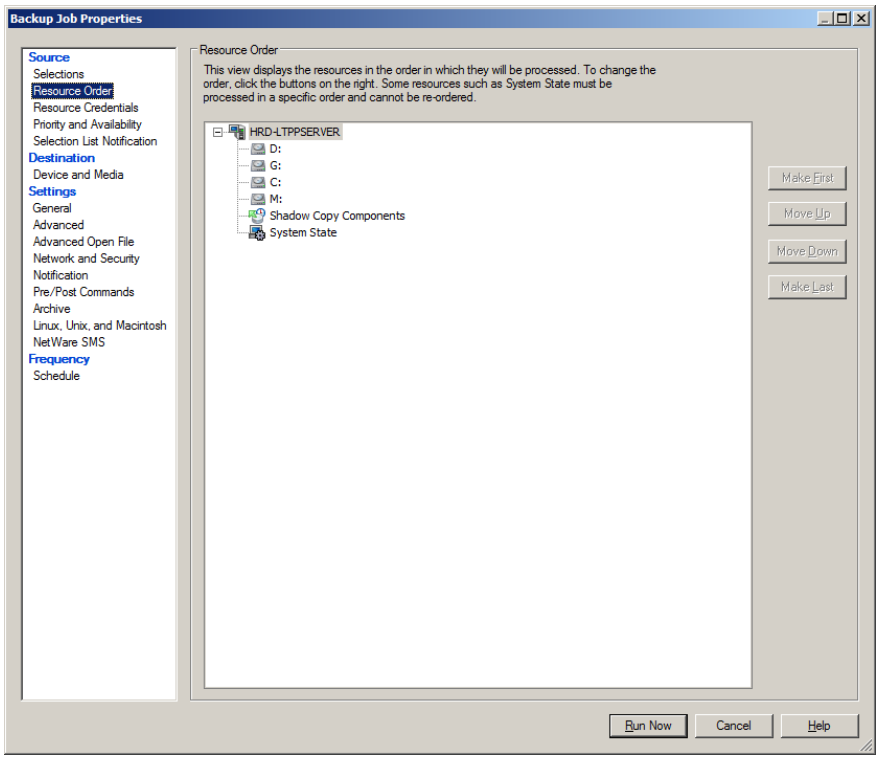


Figure 126. Screenshot. Selecting Resource Order

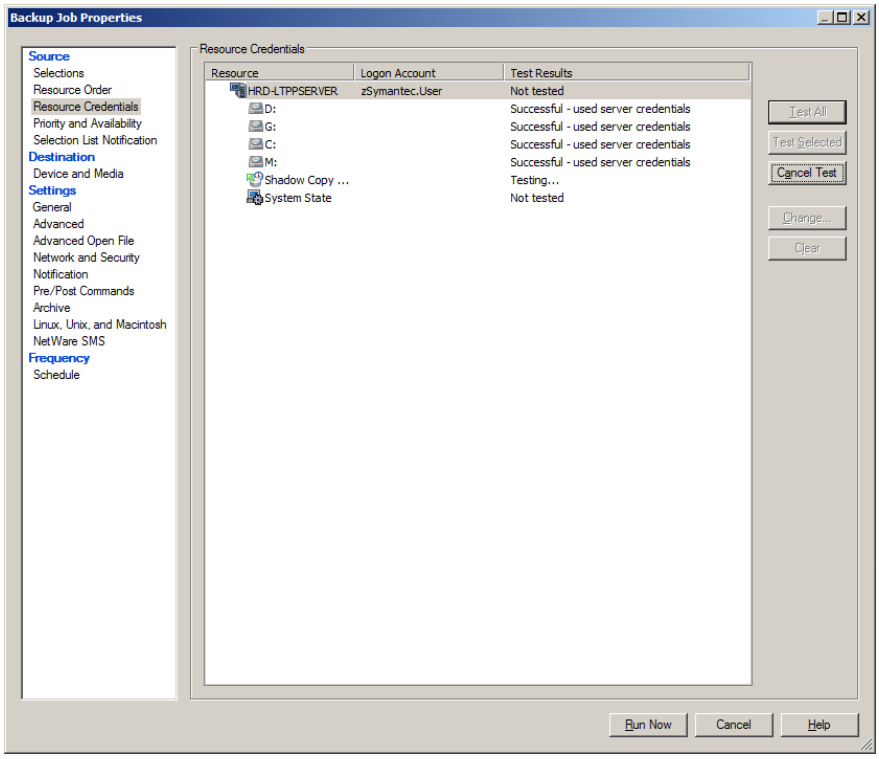


Figure 127. Screenshot. Resource Credential - Testing Log on

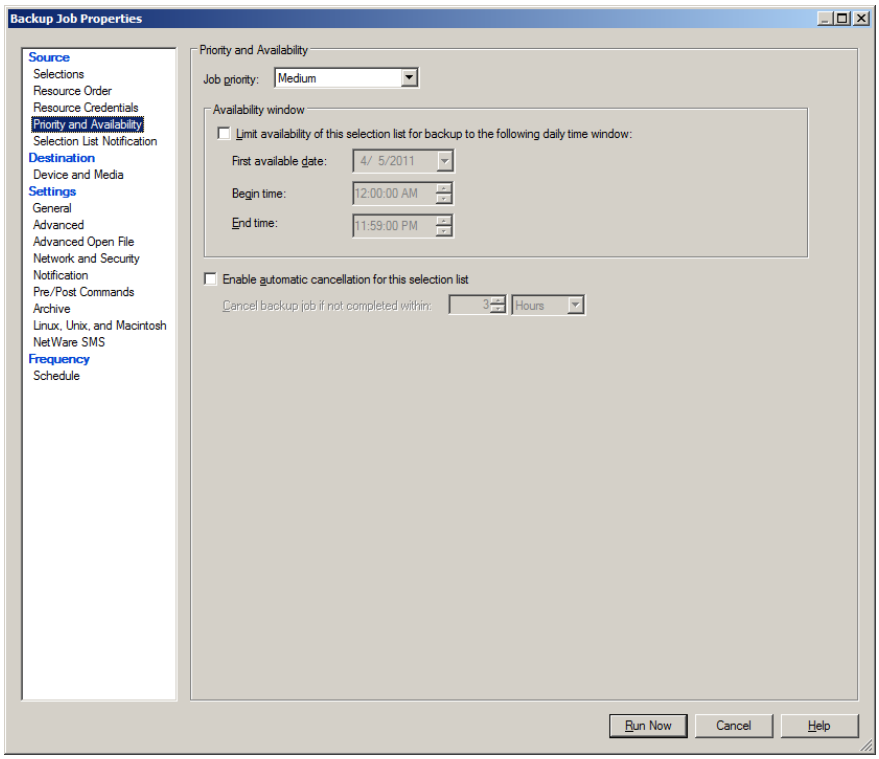


Figure 128. Screenshot. Priority Selection – Defaults

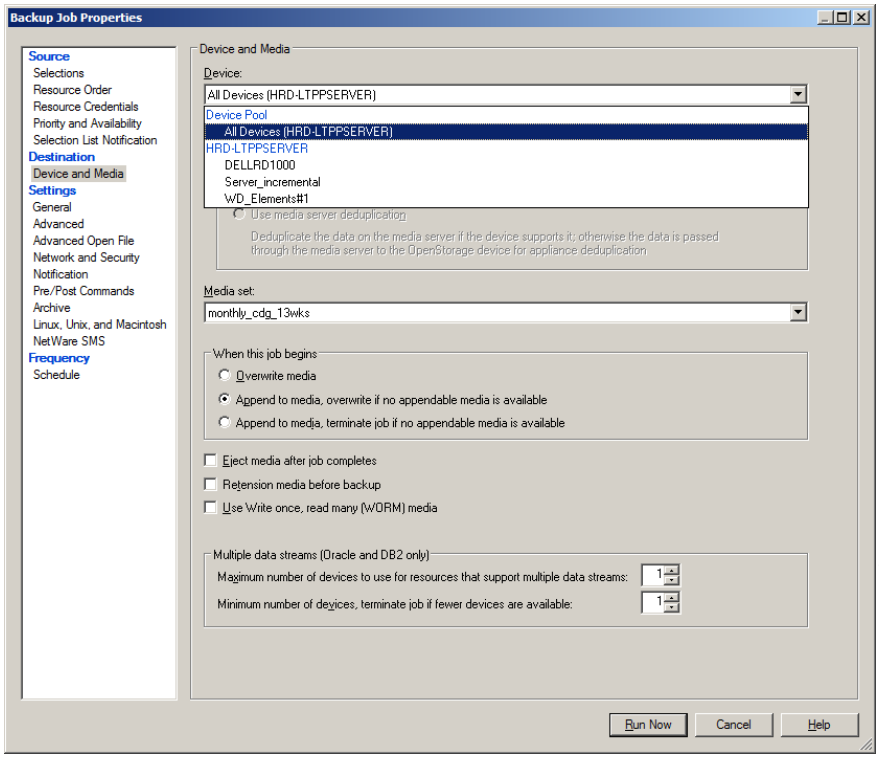


Figure 129. Screenshot. Selecting a Backup Device

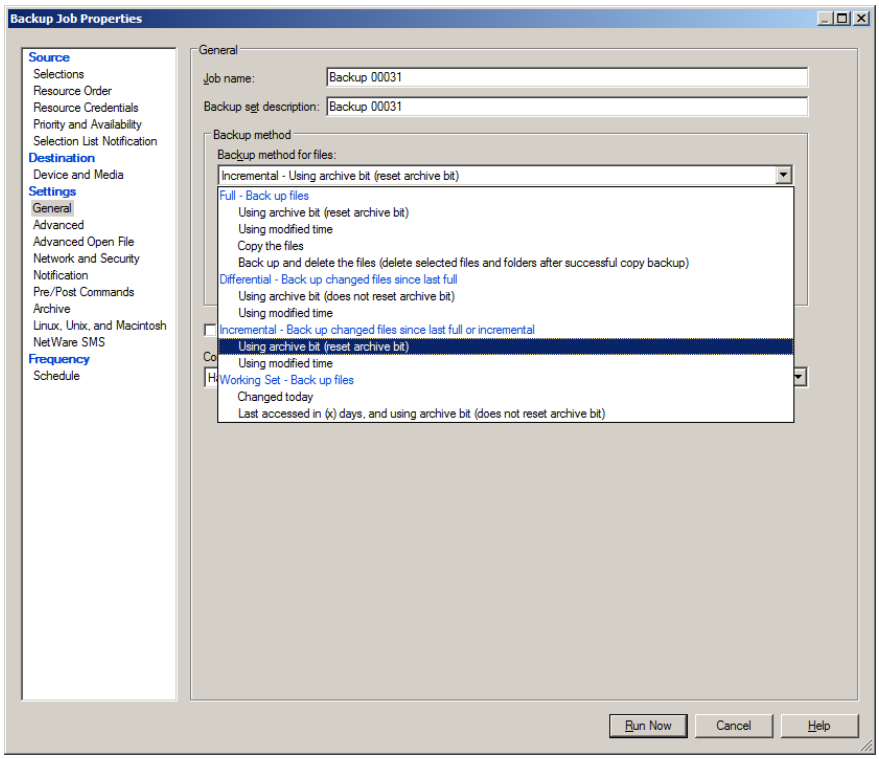


Figure 130. Screenshot. Picking General Settings – Backup Method

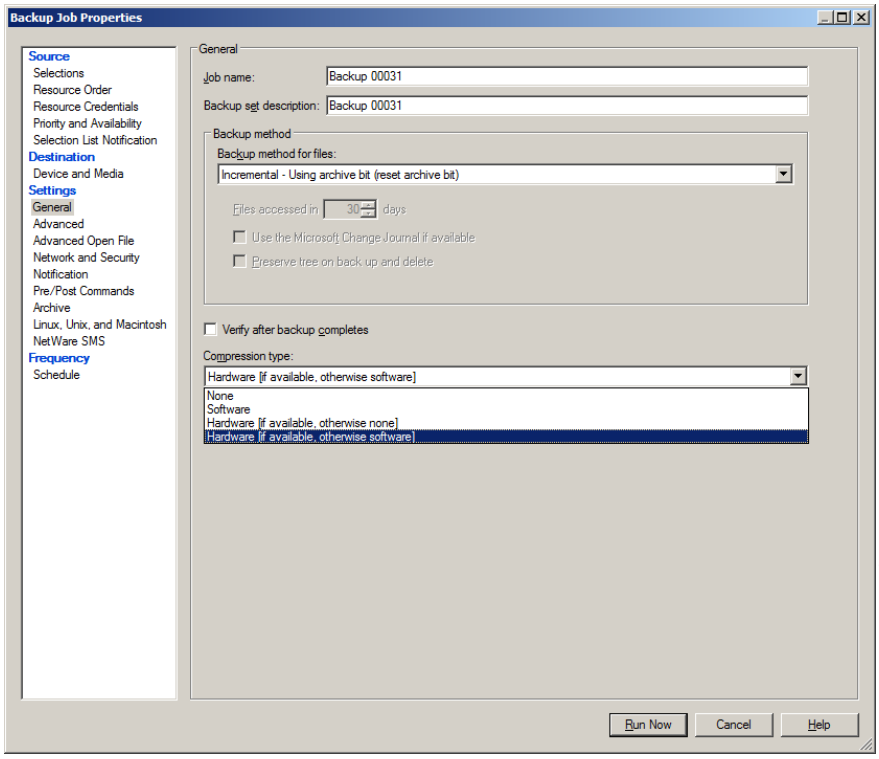


Figure 131. Screenshot. Picking General settings – Compression Type

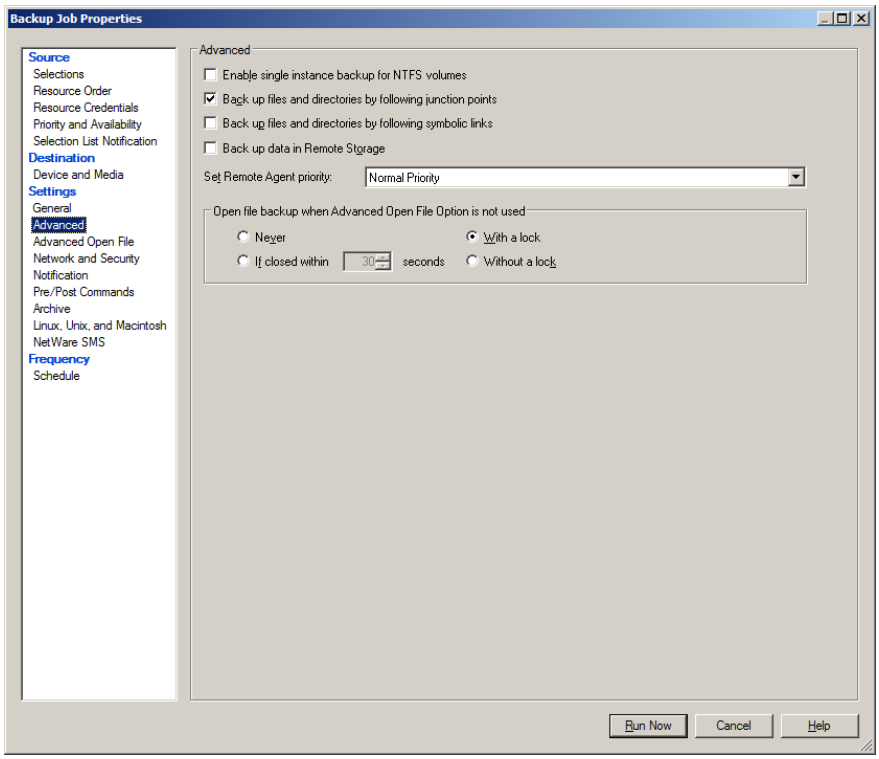


Figure 132. Screenshot. Selection of Advanced Options (Defaults)

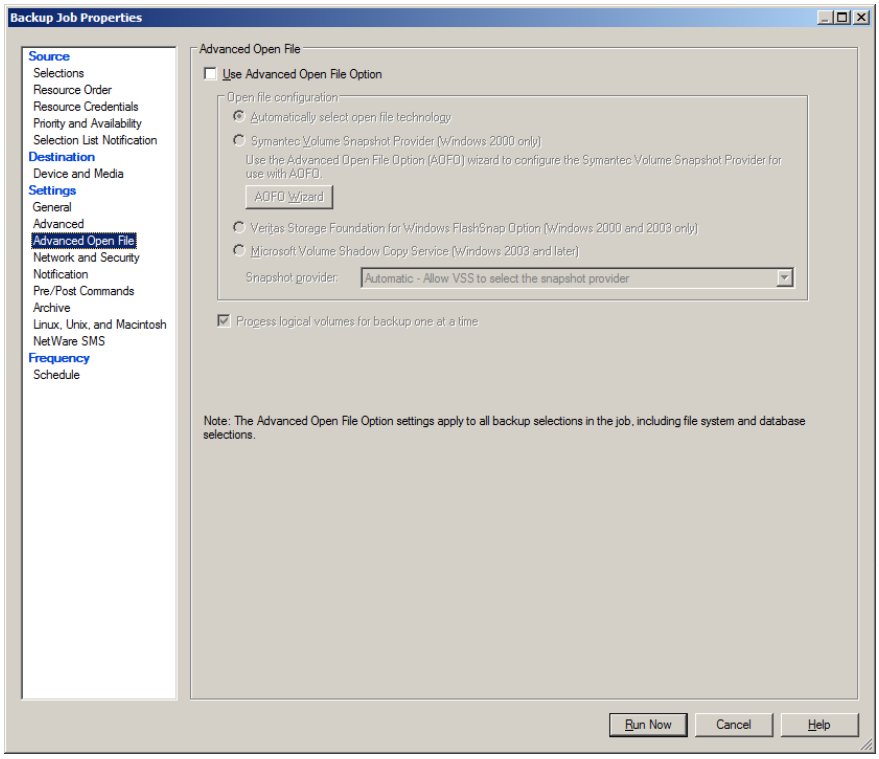


Figure 133. Screenshot. Setting Advanced Open File Options (defaults)

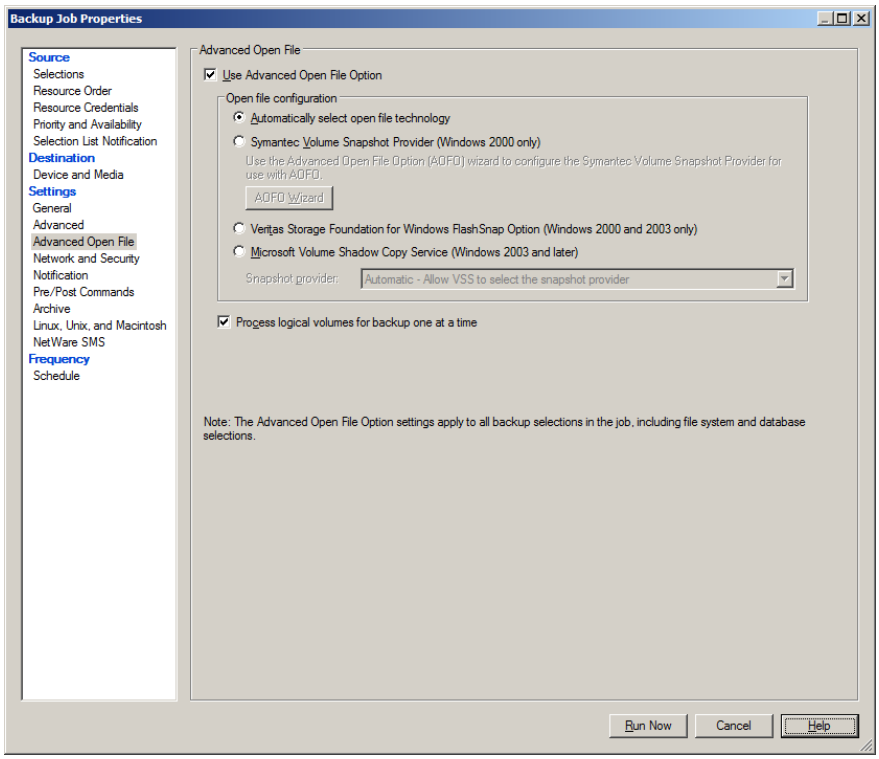


Figure 134. Screenshot. Advanced Open File Options Used

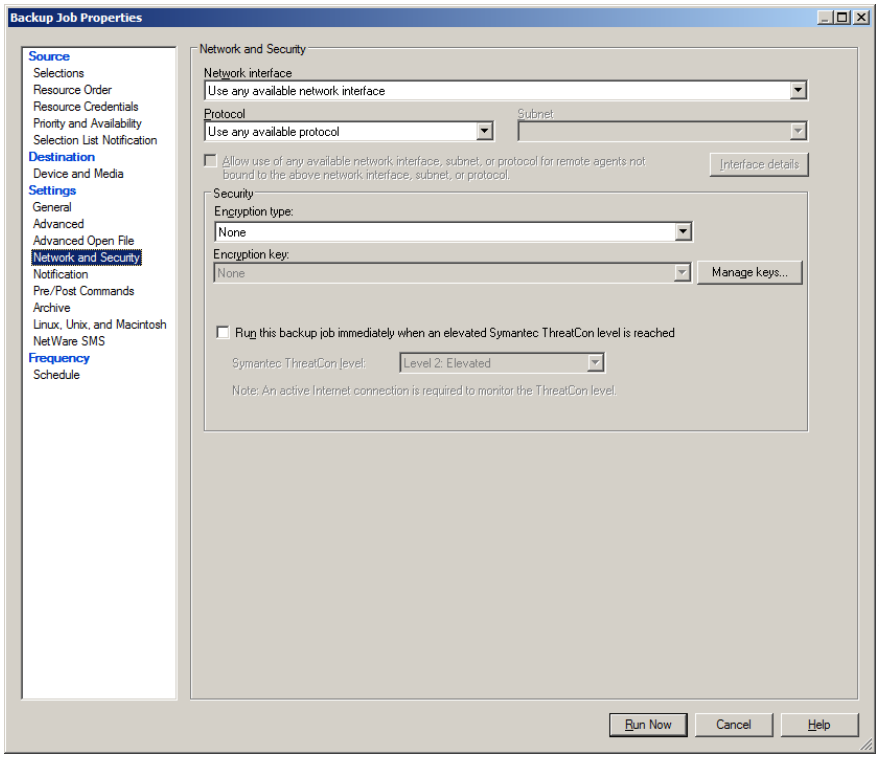


Figure 135. Screenshot. Using Defaults for Network and Security

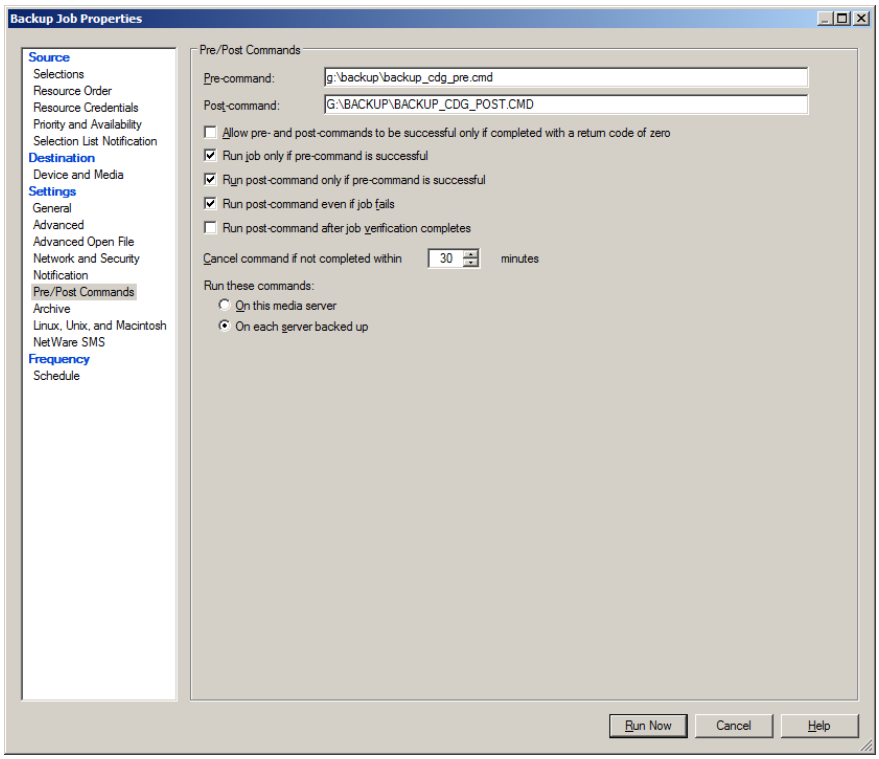


Figure 136. Screenshot. Identifying Pre- and Post- Commands

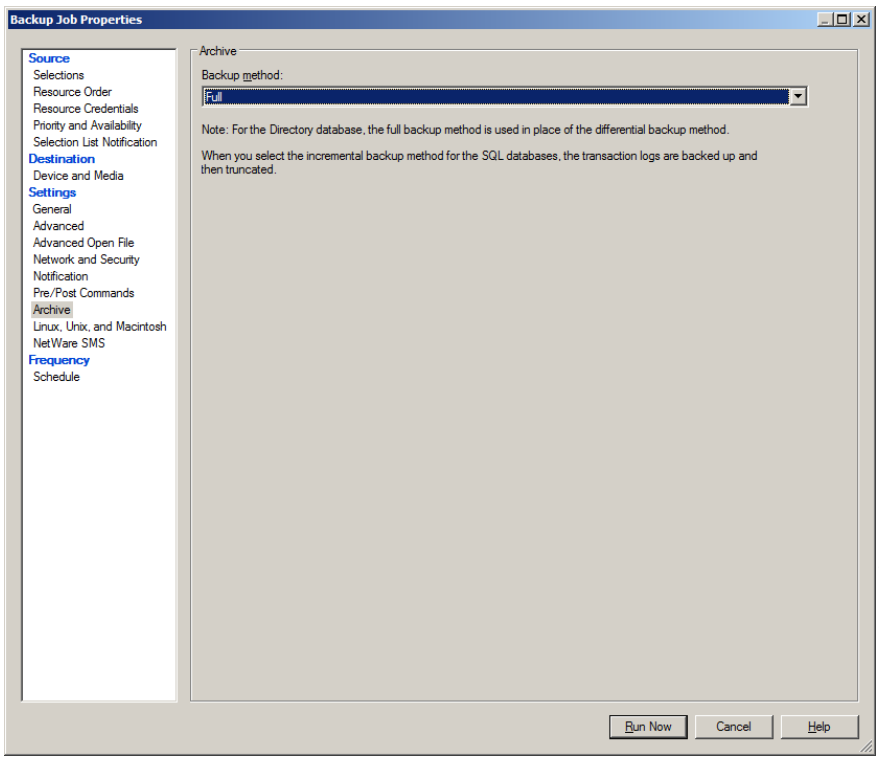


Figure 137. Screenshot. Archive Method Selection

SETTING UP A RECURRING JOB

To set up a recurring job, the same steps of the job set up process as followed with the exception of the schedule selection.

MANAGING JOBS

The upper left box, General Tasks, on the Job Setup screen has several functions that may be useful: Delete, Properties, Run now, and Test run. Copy is a between server function and not applicable to the LTPP system.

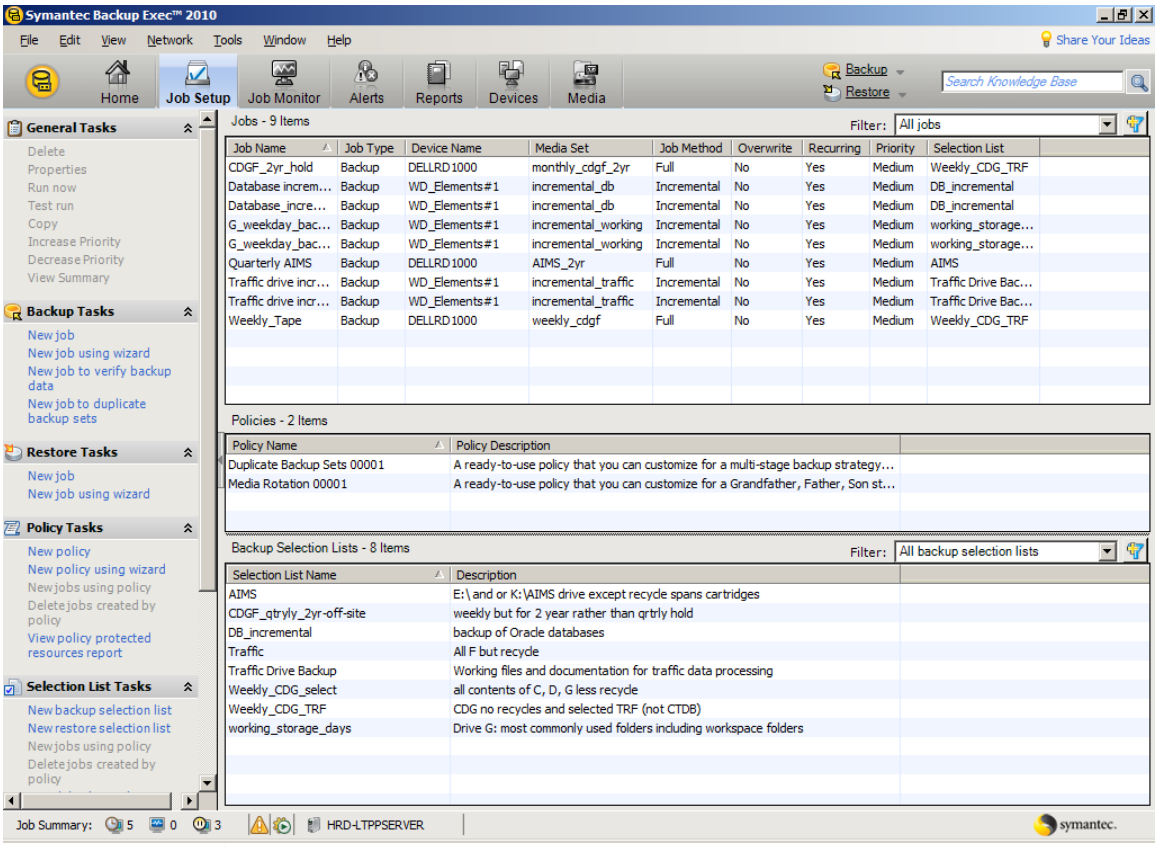


Figure 138. Screenshot. Job functions accessible through Job Setup screen

Delete does exactly what it says, removes a job from the list. Highlight a job and click on it. The response will be the dialog box in figure 44. The selection list option exists to remove the information about what is being backed up. Unless the list is used only for the job or is not anticipated to be used in the future, it should not be deleted.

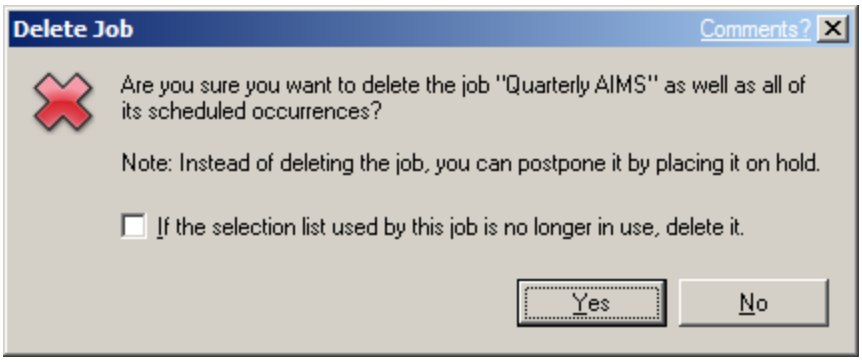


Figure 139. Screenshot. Delete Confirmation dialog box

Selection of a job and clicking on Properties provides the capabilities to edit an existing job. The dialog box in Figure 140 will appear after the selection and click. Any item on the list may be checked and changed if necessary. To save any changes click on "Submit". The revised properties should be saved for reference by creating a pdf in the associated backup log folder.

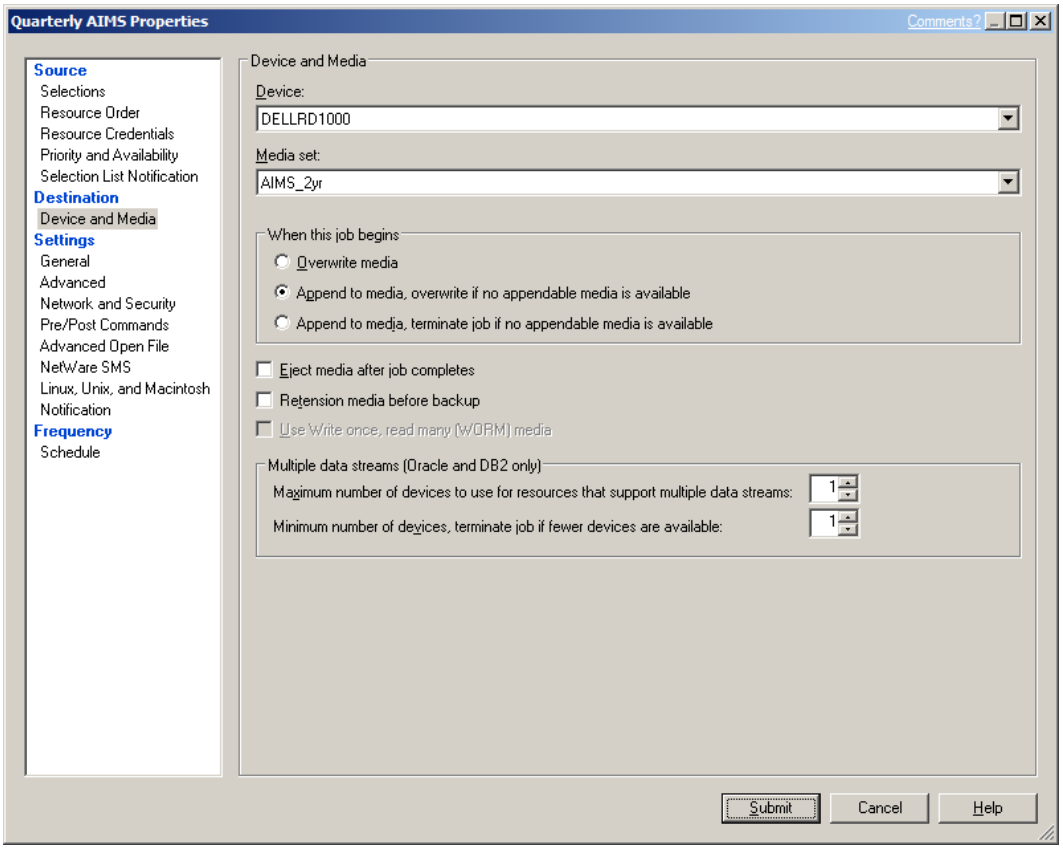


Figure 140. Screenshot. Initial Properties dialog box

The Run now option starts a job immediately rather than waiting for a scheduled time or setting up a schedule.

The Test run function checks that all of the pieces are present, drives accessible to the user, command files for pre and post job actions readable and so forth. It will execute all of the elements of the backup job except the actual backup.

REVIEWING JOB HISTORY

SAVING BACKUP REPORTS

Printed copies of backup reports are created once a week to have a “permanent” record of backups made and their content. Printed copies are made with Adobe Acrobat.

Job reports can be stored indefinitely in BE. These guidelines have been established to set limits on the amount of information stored.

Figure 141 shows a series of folders on drive G:\ (Working Storage) of the server that apply to backups. Included are the folders Backup_logs and Symantec_Backup(Source_Files?). The latter is exactly what it says and is the location for the original software and any patches applied manually.

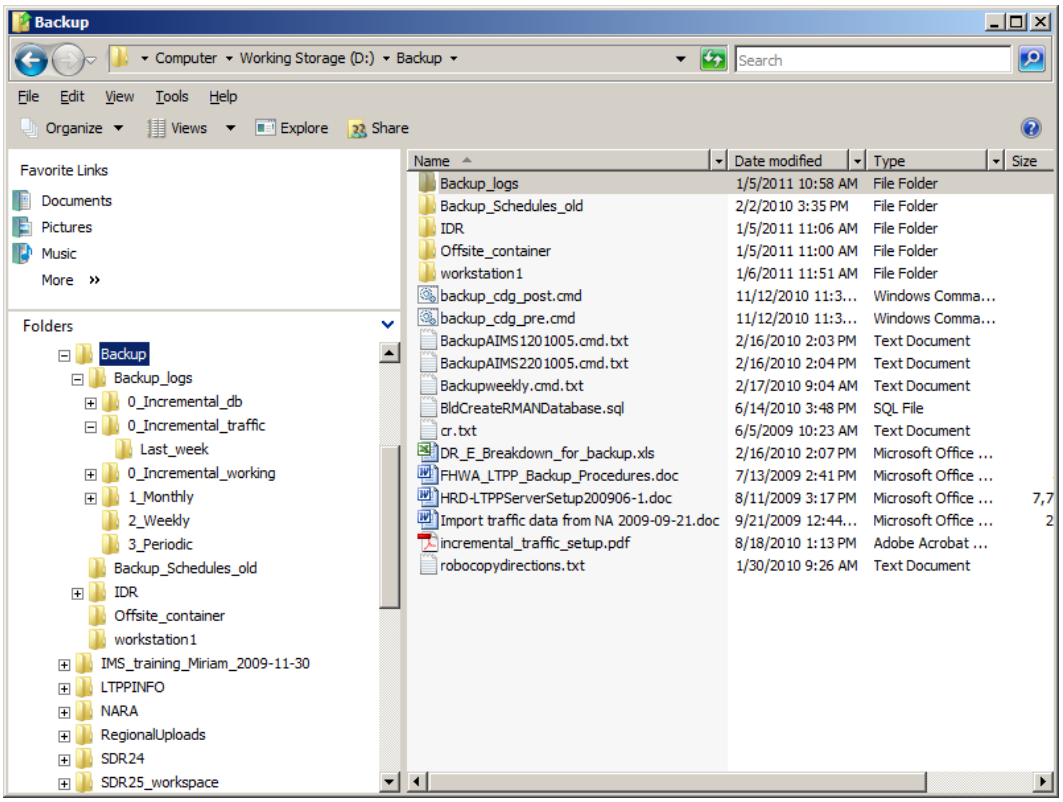


Figure 141. Screenshot. Folders on server for storing backup reports.

The folder Backup has three sub folders: Backup_logs, IDR and Offsite_container. IDR (Intelligent Disaster Recovery) is a folder used by BE. Offsite_container contains files on the original system for storing cartridges off-site. Backup_logs holds all the copies of the backup job set ups, histories and logs.

There are six sub-folders under Backup_logs: 0_Incremental_db, 0_Incremental_traffic, 0_Incremental_working, 1_Monthly, 2_SDR, 3_Weekly, 3_Periodic.

- 0_Incremental_db – incremental backup of the LTPP Oracle databases (G:)
- 0_Incremental traffic – incremental backup of the traffic drive (F:)
- 0_Incremental_working – incremental backup of the working storage drive (D:)
- 1_Monthly – full backups that are stored off-site for either 13 weeks or 2 years
- 2_SDR – full backups
- 3_Weekly – full backups that are retained on site.
- 3_Periodic – Quarterly backups.

A folder contains three types of pdfs: job setups, job histories and job logs. Job setups are the final step of the process in Creating a job. The 0_* folders have a Last_week subfolder to store prior weeks pdfs.

Job histories and Job logs are created as follows:

Select the Job Monitor tab

Select a job in the Job History section

Right click on the job to bring up the menu box as shown in Figure 47. Select the earliest if multiple jobs of the same type have run.

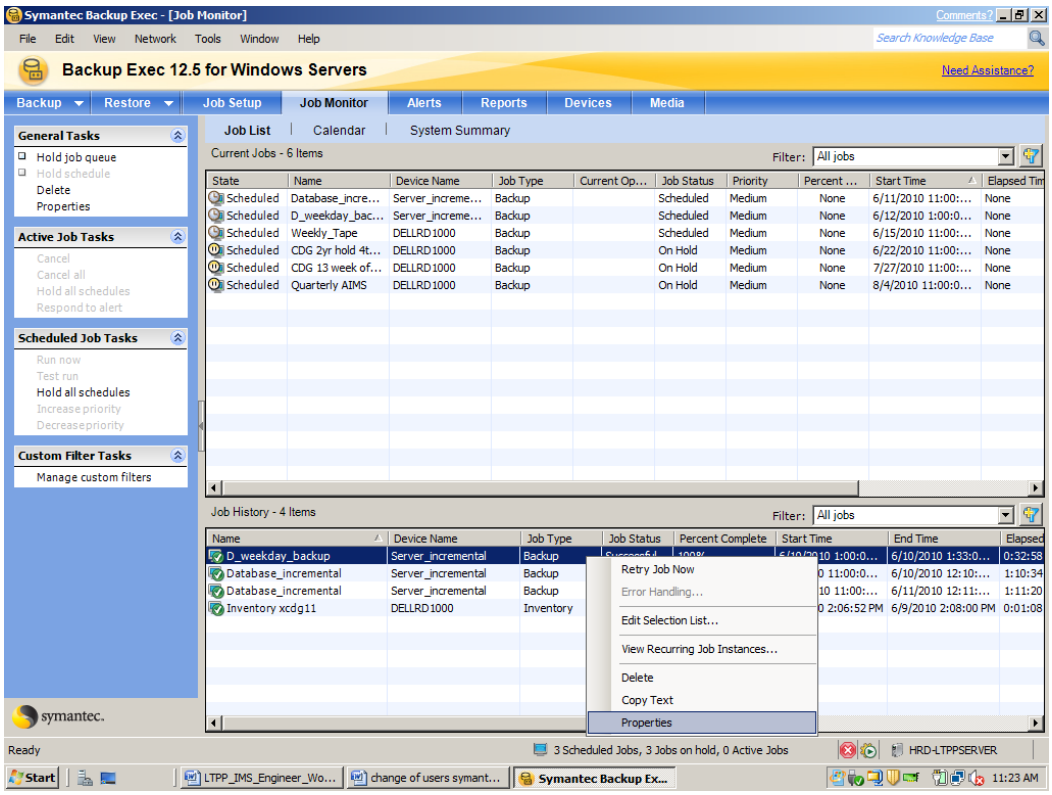


Figure 142. Screenshot. Selecting a Job to Print

Click on Properties.

The Properties selection brings up the Job history screen with its two tabs: Job History and Job Log. Click on Job History The condensed version comes up as shown in Figure 48.

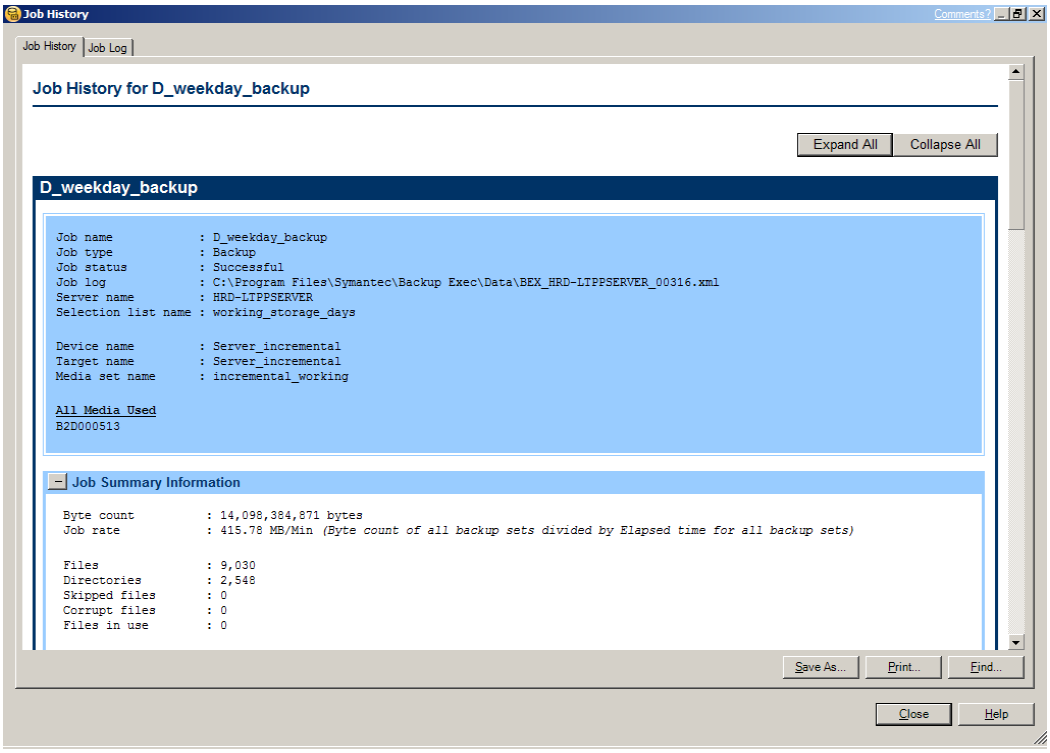


Figure 143. Screenshot. Job History screen.

Click on Job History to ensure it is in front

Click on Expand All (upper right corner)

Click on Print (lower right corner.)

The printer selection menu will come up (Figure 49). Adobe PDF should be the default printer. If not, select it and then click on Print. The filename that comes up is that assigned by BE (Figure 50).

Before changing the file name, verify that the correct directory (Figure 46) in G:\Backup\Backup_logs has been selected.

Enter the file name.

Using the file naming convention, type the first letter of the file name. It can be simpler to edit an existing file name than to type one from scratch. The file name in this case where the Job History tab is forward will be the ‘hist’ version. The dates in the files are the date the backup being printed was STARTED, not the date it finished. If the backup failed, a printout is still made to know which backups do and do not exist. The History or the Log may be missing depending on the type of failure.

The file naming conventions for the various folders are as follows:

- 0_Incremental_weekday – I_work_hist/log_yyyymmdd(_fail)
- 0_Incremental_db – I_db_hist/log_yyyymmdd(_fail)
- 0_Incremental_traffic – I_traffic_hist/log_yyyymmdd(_fail)
- 1_Monthly – cdgfNN_hist/log_yyyymmdd(_fail)
- 2_SDR_>>>>>
- 3_Weekly – cdgfNN_hist/log_yyyymmdd(_fail)
- 3_Periodic – AIMS_tape#_mmyyyy

Click on Save.

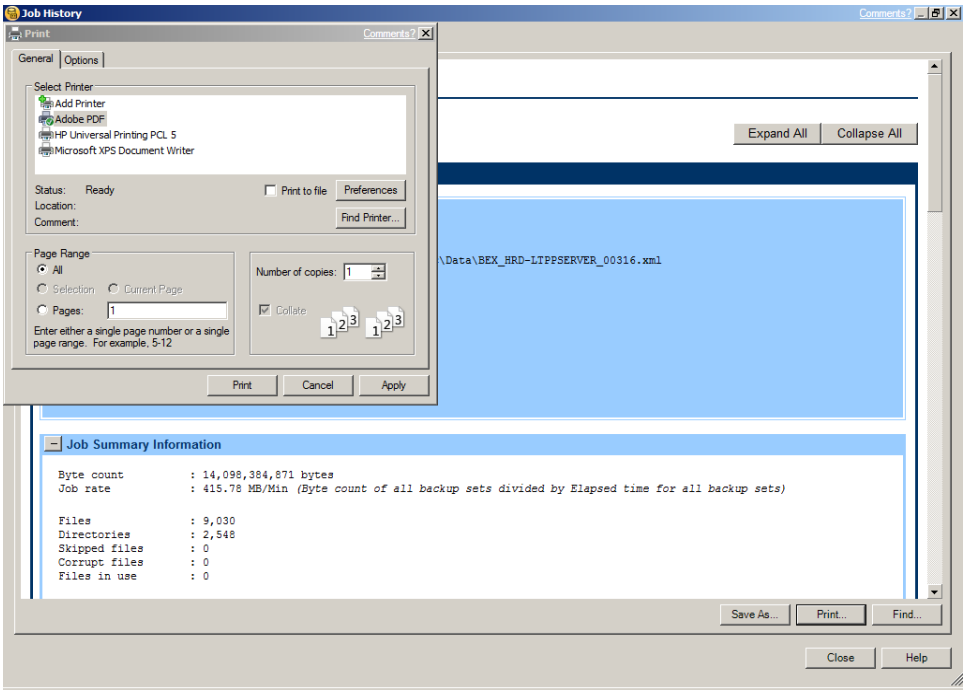


Figure 144. Screenshot. Selecting a Printer.

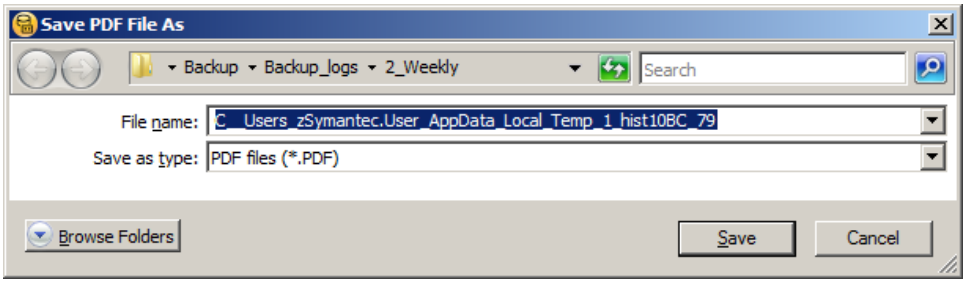


Figure 145. Screenshot. Locations and names for job logs.

Verify the full (expanded) history was printed when it comes up in Acrobat.

Click on Job Log to ensure it is in front (Figure 51).

Click on Expand All (upper right corner)

Click on Print (lower right corner.)

The printer selection menu will come up (Figure 49). Adobe PDF should be the default printer. If not, select it and then click on Print. The filename that comes up is that assigned by BE (Figure 50).

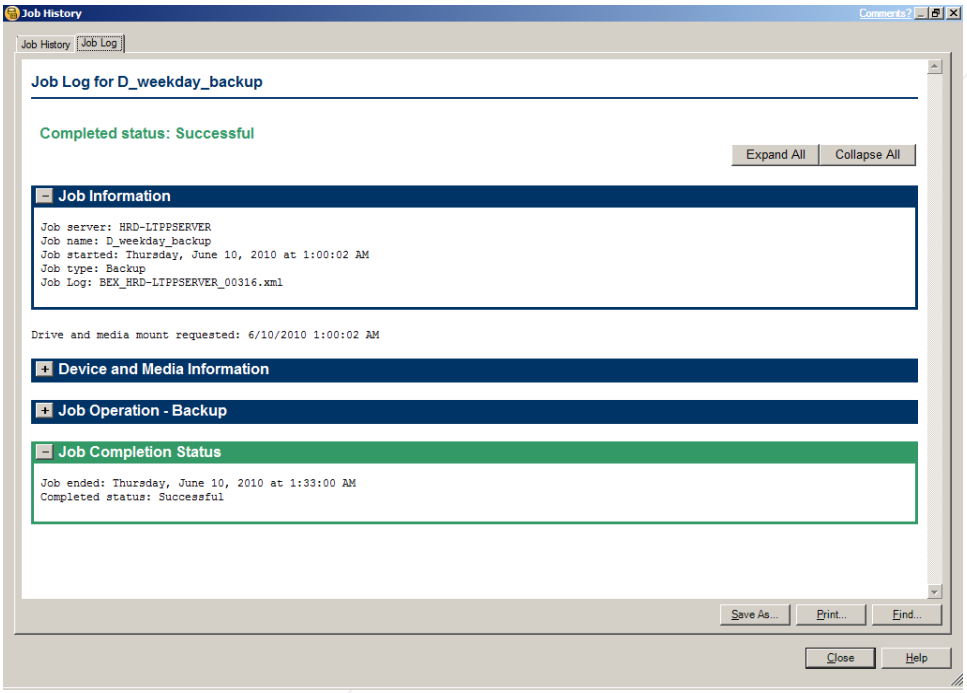


Figure 146. Screenshot. Job Log screen - Summary Form.

Enter the file name.

Type the first letter of the file name. The file name in this case where the Job Log tab is forward will be the ‘log’ version. The dates in the files are the date the backup being printed was STARTED, not the date it finished. If the backup failed, a printout is still made to know which backups do and do not exist. The History or the Log may be missing depending on the type of failure.

Click on Save.

Verify the full (expanded) log was printed when it comes up in Acrobat.

Click on Close.

Return to Symantec and the next Job to be printed.

When all jobs have been printed delete them from the Job History section of Job Monitor.

Add notes on tape replacement; printouts which may not occur

File management discussion: saving; length to hold; length to recycle.

APPENDIX AH. RECOVERY FROM BACKUP – DELL 2900

INTELLIGENT DISASTER RECOVERY

Intelligent Disaster Recovery is the method included in Symantec BE to support file restoration. It has two components, a bootable disk from which the computer can be restarted (or a new one brought up as a replacement) and a tracking system. The bootable disk should be created on at least a yearly basis or after a major system patch. The tracking file should be updated weekly prior to the weekly backup.

PREPARING FOR RECOVERY

On at least a monthly basis after an off-site tape is created a copy of both the disaster recovery file and a bootable image of the primary drive should be updated. The former is referred to as a .dr file in Symantec BE terms. The latter is referenced as an .iso file, an image to be copied to DVD in order to be used. The Dell 2900 has a DVD R drive. The creation of both items is done through the Intelligent Disaster Recovery Preparation Wizard. Both items need to be done to be prepared for recovery.

Select Prepare for (Intelligent) Disaster Recovery in the Job Setup screen once to prepare the .iso file and a second time to create the .dr file.

There may be a User Account control to validate continuing. If so, Click on Continue.

The Wizard will come up. The IDR option has been installed on the server so the block on the screen can remain unchecked before clicking on Next

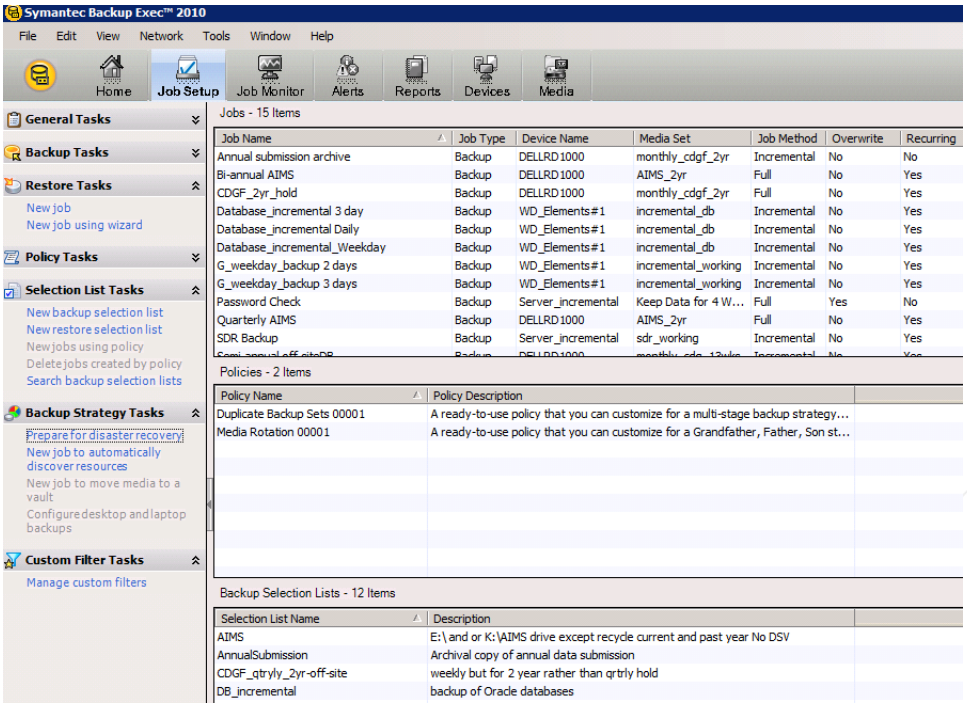


Figure 147. Screenshot. IDR Wizard selection.

Figure 148. Screenshot. IDR Preparation Wizard Opening Screen

IDR Preparation

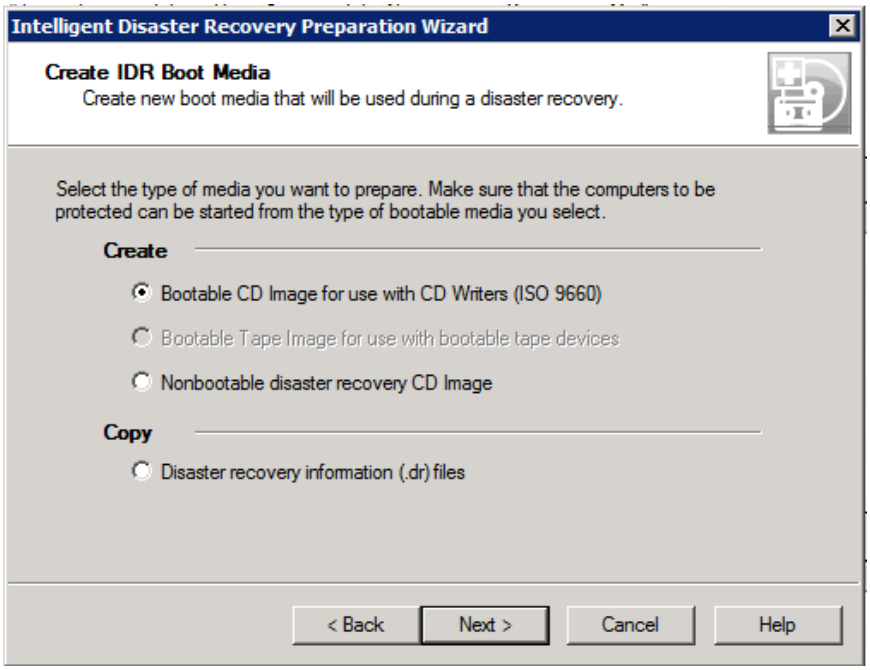


Figure 149. Screenshot. IDR Boot Media Options

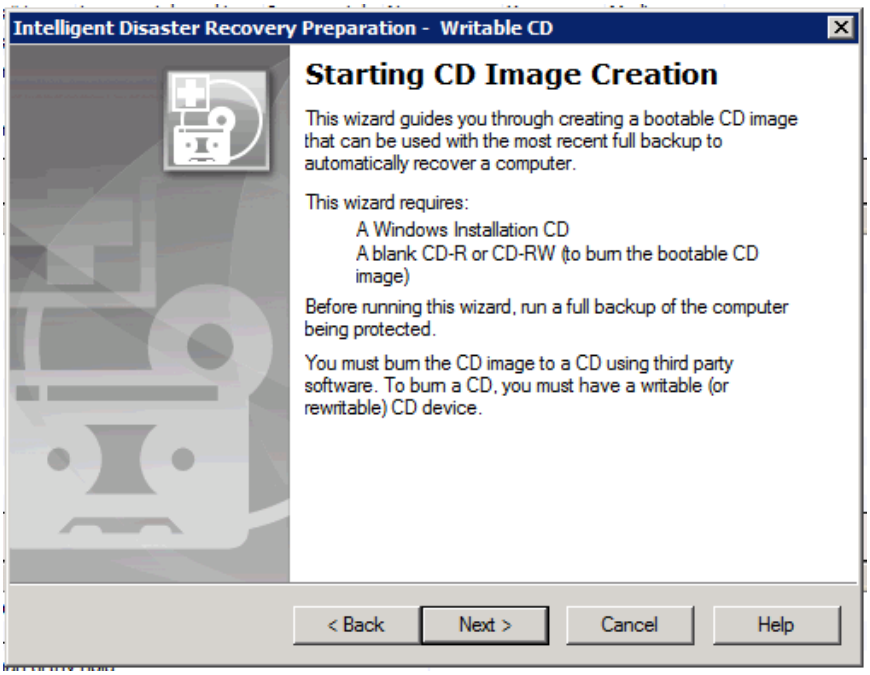


Figure 150. Screenshot. IDR CD Creation Instructions

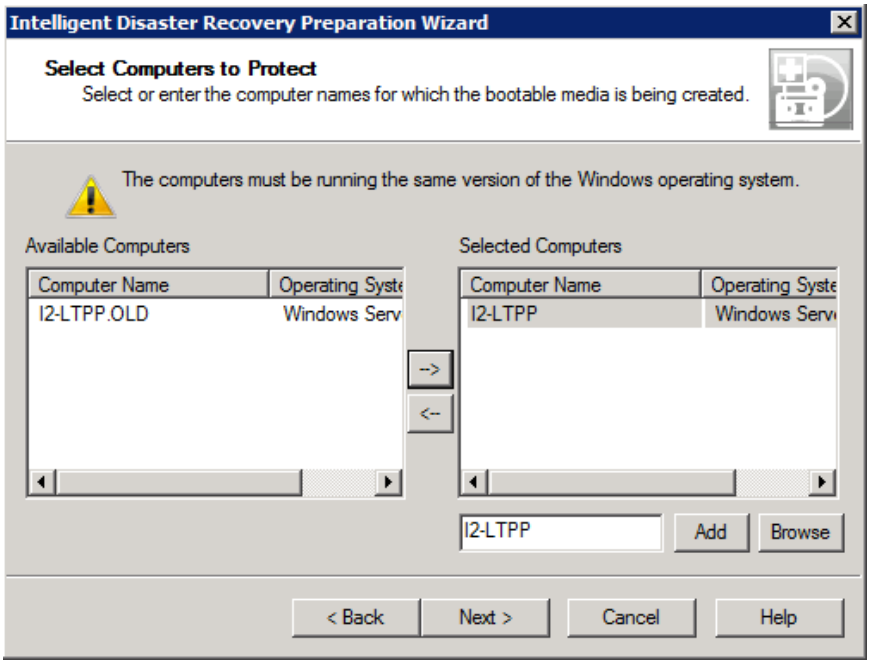


Figure 151. Screenshot. Selecting a computer for disaster recovery preparation.

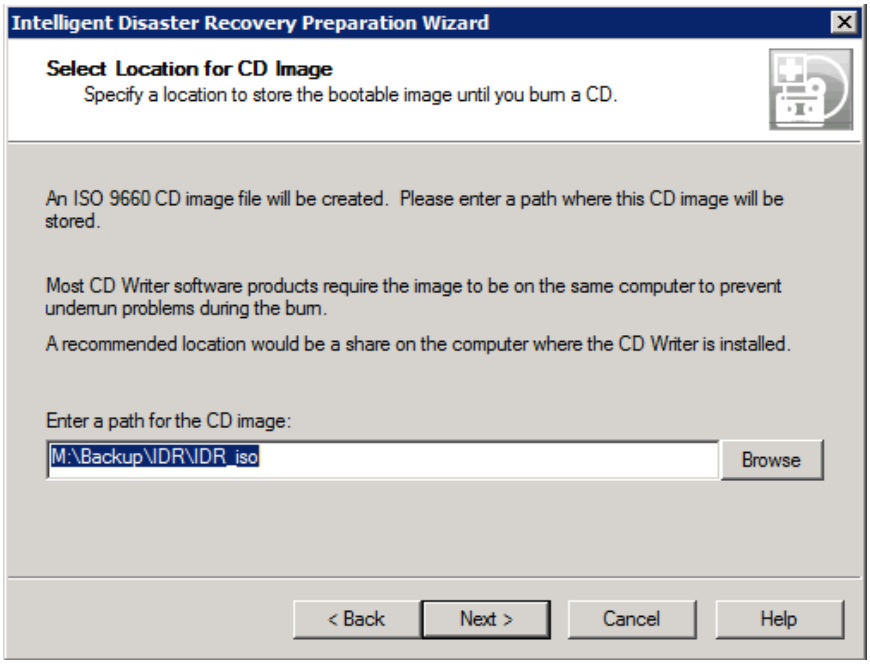


Figure 152. Screenshot. Location selection for CD image.

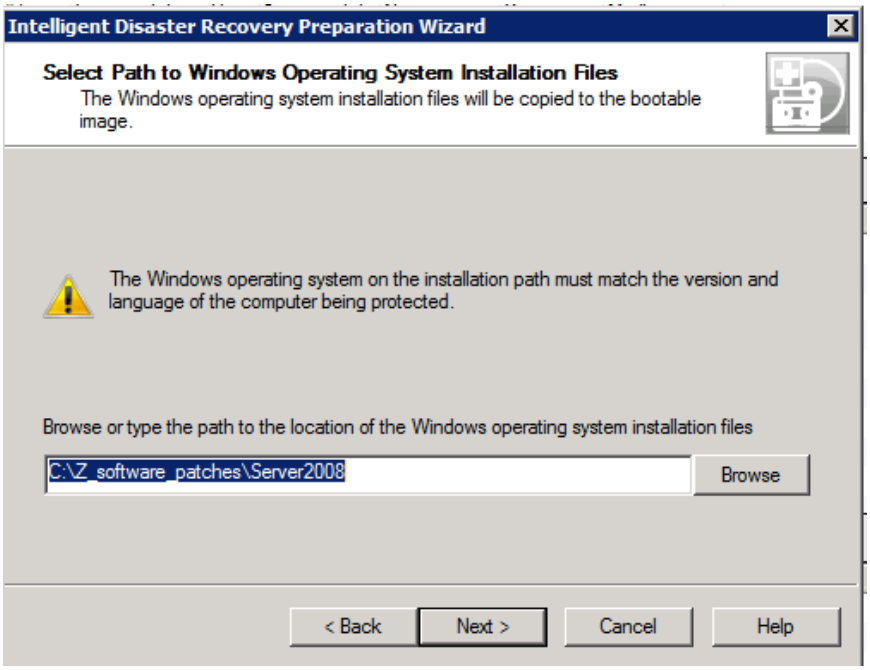


Figure 153. Screenshot. Identifying Windows OS installation file location.

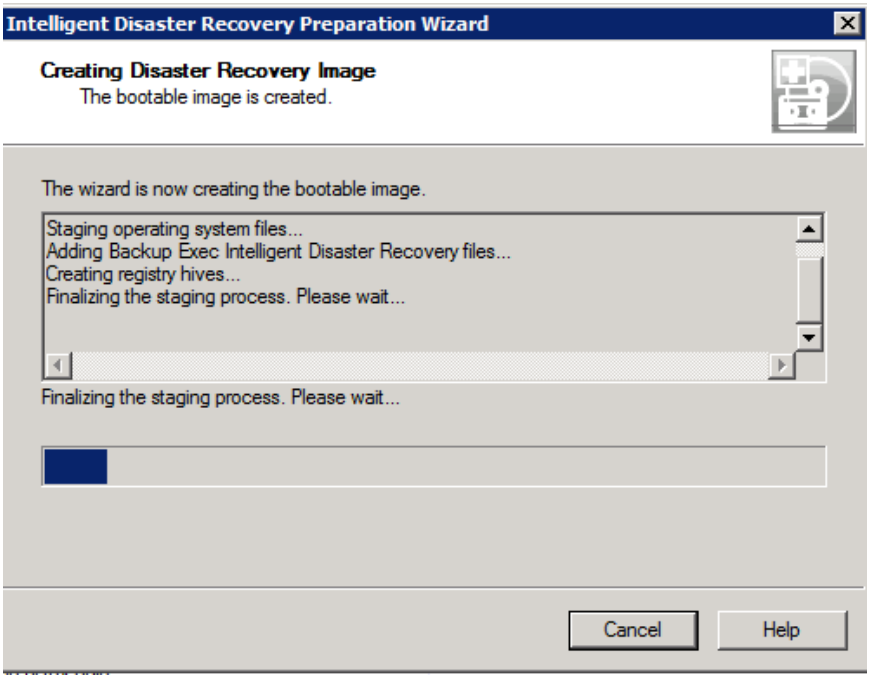


Figure 154. Screenshot. Image creation messages.

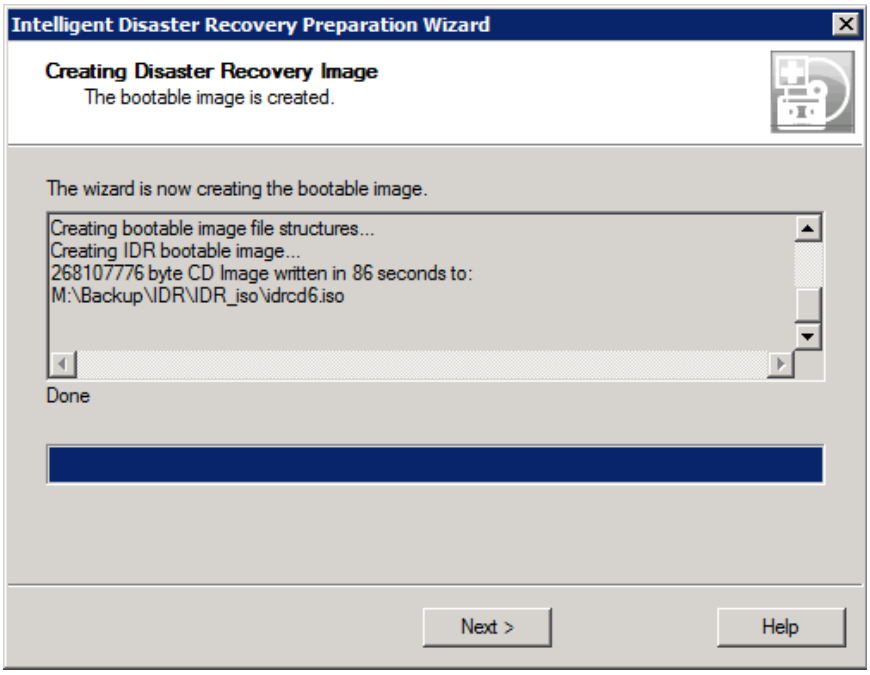


Figure 155. Screenshot. Outcome of disaster recovery preparation.

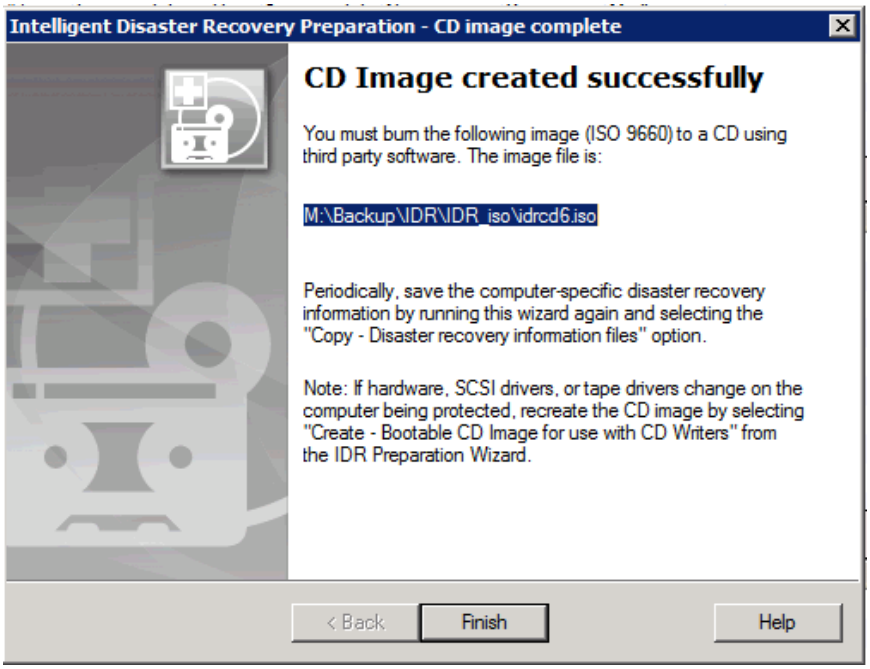


Figure 156. Screenshot. Identification of image file name and location for .iso Files

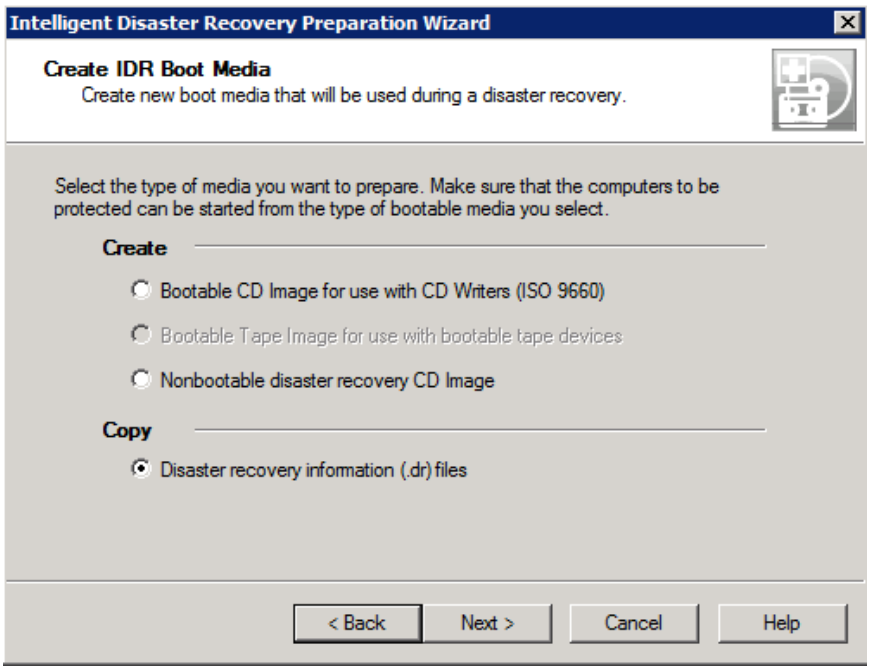


Figure 157. Screenshot. Selecting the Disaster Recovery File Option in the IDR Preparation Wizard

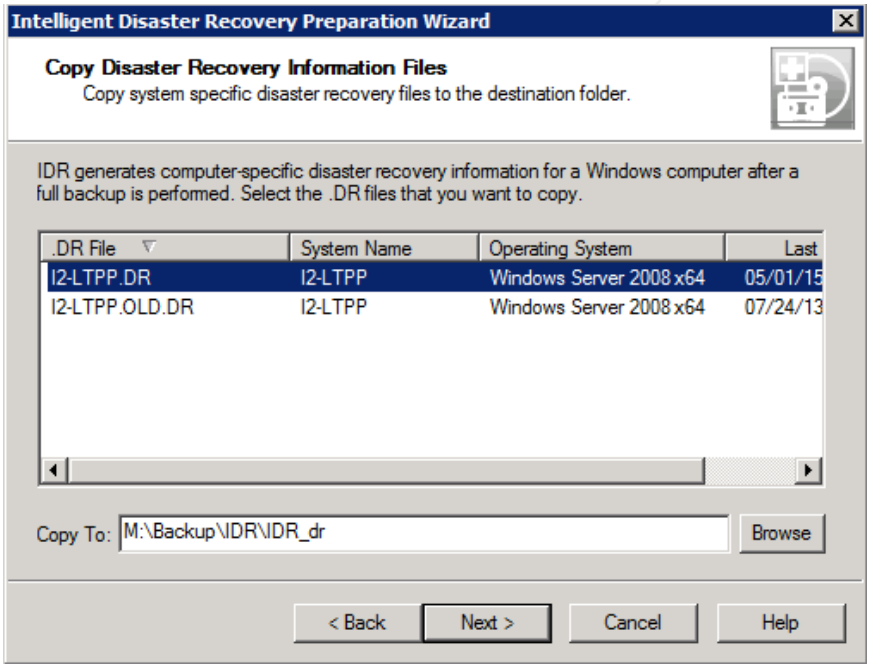


Figure 158. Screenshot. Identifying computer and location for .dr File

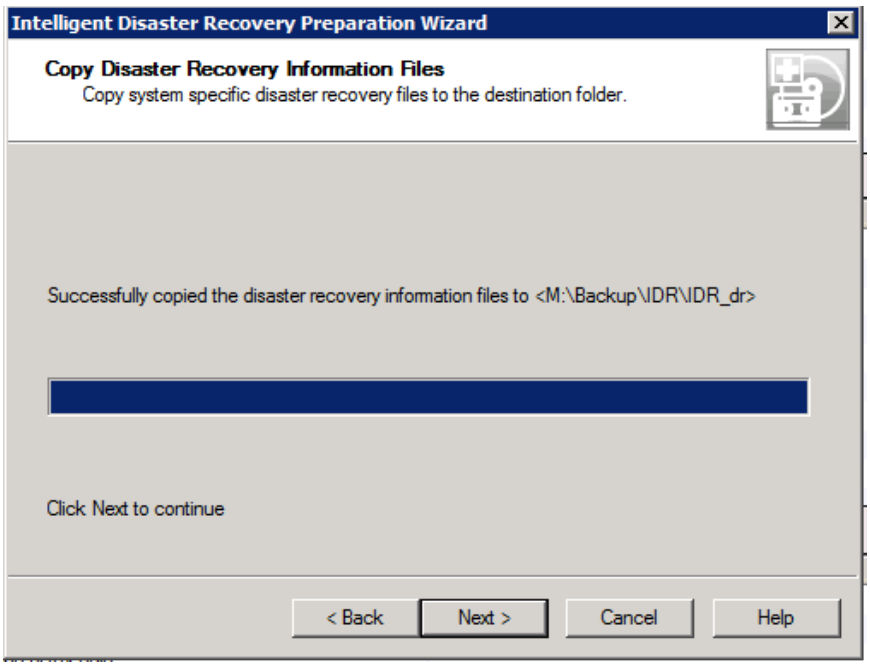


Figure 159. Screenshot. Completion of creation of copy of .dr file.

Figure 160. Screenshot. Completion of disaster recovery preparation.

RESTORING A FILE

APPENDIX AI. ORACLE OPERATIONS – DELL 2900

Basic Oracle syntax does not vary in a material fashion between the two servers. The primary differences between the two TFHRC servers are file locations for Oracle databases and software. This section discusses the Oracle 11g database actions on the Dell 2900.

The Dell 2900 has SQLDeveloper installed. When the central server's version is updated, a copy is made to the Dell 2900 to use in updating. Consistency is only an issue for major version updates (i.e. 3.x to 4.x) so that LTPP documentation updates can be simplified.

BEFORE CLONING TO A NEW INSTANCE

This must be done under the Administrator password on the Dell 2900 to have the necessary privileges.

Since the destination instance did not previously exist a new service will need to be created for it.

Create a new PFILE for the instance by copying an existing pfile. For example, copy initimsprod.ora to initimstest.ora where IMSProd is the existing instance and IMSNew is the new instance.

copy C:\oracle\product\11.2.0\LTPP\database\initimsprod.ora

C:\oracle\product\11.2.0\LTPP\database\initimsnew.ora

If the pfile does not exist, create it from the spfile for the existing instance.

Edit the new PFILE and change "IMSPROD" to "IMSNEW" everywhere using a text editor (Notepad or Notepad ++).

Create the directories for the new instance as indicated with the following syntax ad the command prompt.

```
md D:\LTPP_Database\IMSNew
md D:\LTPP_Database\IMSNew\Trace (verify that trace is located here.
It may be located in d:\LTPP_Database\diag\rdbms\imsnew\trace)
md D:\LTPP_Database\IMSNew\Tablespaces
md D:\LTPP_Database\IMSNew\Modifications
md K:\0_oracle_flash_recovery\11g_new?
```

Create the service for IMSNew at the command prompt using the syntax -

```
oradim –new –sid IMSNew –syspwd sys4imstest –maxusers 50 –startmode
auto –pfile "C:\oracle\product\11.2.0\LTPP\database\initimsnew.ora"
```

The value of syspwd should be recorded for reference. Loss of the SYS password may require deleting and recreating the instance.

Edit C:\oracle\product\11.2.0\LTPP\network\admin\tnsnames.ora. Duplicate the IMSProd entry and change IMSProd to IMSNew in the copy.

Edit C:\oracle\product\11.2.0\LTPP\network\admin\Listener.ora. Duplicate the IMSProd entry and change IMSProd to IMSNew in the copy.

Restart the listener logged in to the Administrator account using the syntax of the next two lines at the command prompt.

```
lsnrctl stop
lsnrctl start
```

CLONING

Cloning is the duplication of a database. Throughout this discussion IMSProd is the source instance being cloned. IMSNew is the instance that is getting and exact duplicate (clone) of IMSProd.

Shut down the source instance to be cloned using the following syntax where each line is a separate entry. The initial line is executed at the command prompt. SQLPlus is called in the first line. The remaining lines are executed at the SQLPlus prompt.

```
sqlplus “sys/syspwd@imsprod as sysdba”
create pfile from spfile;
alter database backup controlfile to trace;
shutdown immediate;
exit;
```

Shut down the destination instance (if not newly created) using the syntax in the next three lines. The first line calls SQLPlus and the remaining lines run at the SQLPlus prompt.

```
sqlplus “sys/syspwd@imsnew as sysdba”
shutdown immediate;
exit;
```

Delete the files from the destination directories. Log on as Administrator to do this without having to check folder permissions. The syntax provided is run at the command prompt rather than using Windows Explorer to do the same thing.

(Check for location of trace files)

```
del D:\LTPP_Database\IMSNew
del D:\LTPP_Database\IMSNew\Modifications
del D:\LTPP_Database\IMSNew\Trace
del D:\LTPP_Database\IMSNew\Tablespaces
```

Copy the source instance to the destination.

```
copy D:\LTPP_Database\IMSProd\*.* D:\LTPP_Database\IMSNew
copy D:\LTPP_Database\IMSProd\Tablespaces\*.*
          D:\LTPP_Database\IMSNew\Tablespaces
```

Create a SQL script to generate a new control file that identifies the clone database name and points to the new file location. Note that once this script is created, these steps only need to be repeated when new data files are added to the database. It is, however, good practice to create a new script every time a database is cloned.

A script to generate a control file is created with the following steps.

1. Find the trace file with the same timestamp as the "alter database backup controlfile to trace" command. This will be located in the source database's trace directory. An example would be "D:\LTPP_Database\IMSProd*Trace-find correct directory* \imsprod_ora_2976.trc".

2. Save the file as "D:\LTPP_Database\IMSNew\Modifications\CreateIMSNewControlFile.sql".

3. Edit the trace file with a text editor, i.e. Notepad++ or Notepad.

    a. Find the "Set #2. RESETLOGS case" section

    b. Delete everything above the "STARTUP NOMOUNT" line

    c. Find the "ALTER TABLESPACE" line and delete everything below it

    d. Find the line with the ; (semi-colon) after CHARACTER SET US7ASCII.

        i. Remove all lines down to ALTER DATABASE OPEN RESETLOGS

        ii. Remove all commented lines (lines beginning --_.

        iii. Remove the line - RECOVER DATABASE USING BACKUP CONTROLFILE

    e. Change all occurrences of "IMSPROD" to "IMSNew" (the new instance name.)

    f. Change path if necessary.

    g. Change the "CREATE CONTROLFILE REUSE DATABASE" line to "CREATE CONTROLFILE REUSE SET DATABASE"

4. Save the file.

The new instance is started by

- Executing the script to create the control file from the SQLPlus prompt.
- Changing user passwords
- Deleting LTPP created users not used in the instance.
- Adding the instance specific users. This is best done with scripts if object level privileges are granted.
- Creating a SPFILE and restart the database instance using it.

The sequence of commands from the command prompt is typically –

```
sqlplus “sys/syspwd@imsnew as sysdba”
```

Followed by a series of command executed at the SQLPlus prompt.

```
(if connected to an idle instance - Shutdown abort;)
@D:\LTPP_Database\CreateIMSTestControlFile.sql
Alter user ltppdba identified by newpwd replace oldpwd (cloned db);
Alter user trfdba identified by newpwd replace oldpwd;
Alter user custsupp identified by newpwd replace oldpwd (cloned db);
Alter user system identified by newpwd replace oldpwd (cloned db);
Alter user datacheck identified by newpwd replace oldpwd;
Drop originatingInstanceUser on delete cascade;
Create NewInstanceUser identified by userpwd
      Default tablespace user_data
      Temporary tablespace temporary_ts;
Grant power_user to NewInstanceUser;
Grant select_only to datacheck identified by datacheckpwd;
shutdown immediate;
create spfile from pfile;
startup;
```

Connect to the database from which the clone was made and start it.

```
Connect sys/syspwd@imsprod as sysdba
Startup open;
Exit;
```

If the listener does not know of the service when the attempt is made to log on do the following at the command prompt:

```
Lsnrctl stop
Lsnrctl start
```

APPENDIX AJ. ROBOCOPY SYNTAX

Prior to acquisition of Backup Exce the Dell 2900 used Robocopy as the backup tool. Since the annual submissions saved in that format have not been verified as replaced on the central server, the syntax is provided here for easy reference.

Robocopy is a Windows utility for making copies. The following lists all of the switches and their actions for the utility.

```
-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Sat Jan 30 09:26:21 2010

              Usage :: ROBOCOPY source destination [file [file]...] [options]

             source :: Source Directory (drive:\path or \\server\share\path).
        destination :: Destination Dir  (drive:\path or \\server\share\path).
               file :: File(s) to copy  (names/wildcards: default is "*.*").

::
:: Copy options :
::
                 /S :: copy Subdirectories, but not empty ones.
                 /E :: copy subdirectories, including Empty ones.
             /LEV:n :: only copy the top n LEVels of the source directory tree.

                 /Z :: copy files in restartable mode.
                 /B :: copy files in Backup mode.
                /ZB :: use restartable mode; if access denied use Backup mode.
            /EFSRAW :: copy all encrypted files in EFS RAW mode.

  /COPY:copyflag[s] :: what to COPY for files (default is /COPY:DAT).
                       (copyflags : D=Data, A=Attributes, T=Timestamps).
                       (S=Security=NTFS ACLs, O=Owner info, U=aUditing info).

           /DCOPY:T :: COPY Directory Timestamps.

               /SEC :: copy files with SECurity (equivalent to /COPY:DATS).
            /COPYALL :: COPY ALL file info (equivalent to /COPY:DATSOU).
             /NOCOPY :: COPY NO file info (useful with /PURGE).

             /SECFIX :: FIX file SECurity on all files, even skipped files.
             /TIMFIX :: FIX file TIMes on all files, even skipped files.

              /PURGE :: delete dest files/dirs that no longer exist in source.
                /MIR :: MIRror a directory tree (equivalent to /E plus /PURGE).

                /MOV :: MOVe files (delete from source after copying).
               /MOVE :: MOVE files AND dirs (delete from source after copying).

     /A+:[RASHCNET] :: add the given Attributes to copied files.
     /A-:[RASHCNET] :: remove the given Attributes from copied files.

             /CREATE :: CREATE directory tree and zero-length files only.
                /FAT :: create destination files using 8.3 FAT file names only.
                /256 :: turn off very long path (> 256 characters) support.
```

```
             /MON:n :: MONitor source; run again when more than n changes seen.
             /MOT:m :: MOnitor source; run again in m minutes Time, if changed.

      /RH:hhmm-hhmm :: Run Hours - times when new copies may be started.
                /PF :: check run hours on a Per File (not per pass) basis.

             /IPG:n :: Inter-Packet Gap (ms), to free bandwidth on slow lines.

                /SL:: copy symbolic links versus the target.
::
:: File Selection Options :
::
                 /A :: copy only files with the Archive attribute set.
                 /M :: copy only files with the Archive attribute and reset it.
    /IA:[RASHCNETO] :: Include only files with any of the given Attributes set.
    /XA:[RASHCNETO] :: eXclude files with any of the given Attributes set.

 /XF file [file]... :: eXclude Files matching given names/paths/wildcards.
 /XD dirs [dirs]... :: eXclude Directories matching given names/paths.

               /XC :: eXclude Changed files.
               /XN :: eXclude Newer files.
               /XO :: eXclude Older files.
               /XX :: eXclude eXtra files and directories.
               /XL :: eXclude Lonely files and directories.
               /IS :: Include Same files.
               /IT :: Include Tweaked files.

             /MAX:n :: MAXimum file size - exclude files bigger than n bytes.
             /MIN:n :: MINimum file size - exclude files smaller than n bytes.

          /MAXAGE:n :: MAXimum file AGE - exclude files older than n days/date.
          /MINAGE:n :: MINimum file AGE - exclude files newer than n days/date.
          /MAXLAD:n :: MAXimum Last Access Date - exclude files unused since n.
          /MINLAD:n :: MINimum Last Access Date - exclude files used since n.
                       (If n < 1900 then n = n days, else n = YYYYMMDD date).

                /XJ :: eXclude Junction points. (normally included by default).

               /FFT :: assume FAT File Times (2-second granularity).
               /DST :: compensate for one-hour DST time differences.

               /XJD :: eXclude Junction points for Directories.
               /XJF :: eXclude Junction points for Files.

::
:: Retry Options :
::
               /R:n :: number of Retries on failed copies: default 1 million.
               /W:n :: Wait time between retries: default is 30 seconds.

               /REG :: Save /R:n and /W:n in the Registry as default settings.

               /TBD :: wait for sharenames To Be Defined (retry error 67).

::
:: Logging Options :
::
                /L :: List only - don't copy, timestamp or delete any files.
                /X :: report all eXtra files, not just those selected.
                /V :: produce Verbose output, showing skipped files.
               /TS :: include source file Time Stamps in the output.
               /FP :: include Full Pathname of files in the output.
```

```
              /BYTES :: Print sizes as bytes.

                 /NS :: No Size - don't log file sizes.
                 /NC :: No Class - don't log file classes.
                /NFL :: No File List - don't log file names.
                /NDL :: No Directory List - don't log directory names.

                 /NP :: No Progress - don't display % copied.
                /ETA :: show Estimated Time of Arrival of copied files.

           /LOG:file :: output status to LOG file (overwrite existing log).
          /LOG+:file :: output status to LOG file (append to existing log).

        /UNILOG:file :: output status to LOG file as UNICODE (overwrite existing
log).
       /UNILOG+:file :: output status to LOG file as UNICODE (append to existing
log).

                /TEE :: output to console window, as well as the log file.

                /NJH :: No Job Header.
                /NJS :: No Job Summary.

            /UNICODE :: output status as UNICODE.

::
:: Job Options :
::
        /JOB:jobname :: take parameters from the named JOB file.
       /SAVE:jobname :: SAVE parameters to the named job file
               /QUIT :: QUIT after processing command line (to view parameters).
               /NOSD :: NO Source Directory is specified.
               /NODD :: NO Destination Directory is specified.
                 /IF :: Include the following Files.
```

AIMS backup were made using the following two batch files: BackupAIMS1yyyyMM.cmd and BackupAIMS2yyyyMM.cmd. Each batch file was structured to format and name the cartridge and then copy folders so that the maximum amount of space would be used on the cartridge. A log file was created for each folder backed up.

BackupAIMS1yyyyMM.cmd:

Format J: /V:AIMS1100505 /FS:NTFS /C /Q /X <d:\backup\cr.txt

J:

cd j:\

mkdir AIMS_2008_06

RoboCopy E:\AIMS_2008_06 J:\AIMS_2008_06 /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS12008_Backup_20100505.log

cd j:\

mkdir AIMS_TRACKER

RoboCopy E:\AIMS_TRACKER J:\AIMS_TRACKER /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS1TRKR_Backup_20100505.log

cd j:\

mkdir SDR24

RoboCopy E:\SDR24 J:\SDR24 /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS1SDR24_Backup_20100505.log

cd J:\

mkdir regionaluploads

RoboCopy E:\regionaluploads J:\regionaluploads /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS1regup_Backup_20100505.log

cd J:\

mkdir CTDB

RoboCopy E:\CTDB J:\CTDB /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS1CTDB_Backup_20100505.log

D:

BackupAIMS2yyyyMM.cmd:

Format J: /V:AIMS2100506 /FS:NTFS /C /Q /X <d:\backup\cr.txt

J:

mkdir Installation

RoboCopy E:\Installation J:\Installation /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2Inst_Backup_20100506.log

cd J:\

mkdir AIMS_2009_09

RoboCopy E:\AIMS_2009_09 J:\AIMS_2009_09 /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2_Backup_20100506.log

cd J:\

mkdir ims_uploads

RoboCopy E:\ims_uploads J:\ims_uploads /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2IMSup_Backup_20100506.log

cd J:\

mkdir Installation_200708

RoboCopy E:\Installation_200708 J:\Installation_200708 /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2Inst07_Backup_20100506.log

cd J:\

mkdir old_installation

RoboCopy E:\old_installation J:\old_installation /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2oldInst_Backup_20100506.log

cd J:\

mkdir old_server

RoboCopy E:\old_server J:\old_server /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_AIMS2oldsvr_Backup_20100506.log

D:

The weekly backup was done with the file - backupweekly.cmd. Its contents follow. The structure is to stop the Oracle instances; format the cartridge to be used and name it in the process; create the folder into which the files will be copied, make the copy, write out a log on the folder copied and go on to the next folder. After all folders were copied the Oracle instance were restarted.

The folders copied were C:\ (operating system); D:\(working storage) and G:\(LTPP Database). The Recycle Bin and selected files were omitted from the copies for each folder.

```
Net stop OracleServiceIMSProd
Net stop OracleServiceIMSDev
Net stop OracleServiceIMSTest
Net stop OracleServiceTRFProd
Net stop OracleServiceTRFDev
Net stop OracleServiceTRFTest
```

Net stop OracleServiceTrf09Aug

Format J: /V:CDG100202 /FS:NTFS /C /Q /X <d:\backup\cr.txt

J:

mkdir G_LTPP_Database

RoboCopy G:\ J:\G_LTPP_Database /MIR /NP /R:10 /W:10 /XJ /XF *.bak *.tmp /XD $recycle.bin /LOG:d:\Dr_G_LTPP_DB_Backup_20100216.log

cd j:\

mkdir D_Working

RoboCopy D:\ J:\D_Working /MIR /NP /R:10 /W:10 /XJ /XF pagefile.sys *.bak *.tmp /XD IMS_Training_Miriam_2009-11-30 $recycle.bin system?volume?information /LOG:d:\Dr_D_Work_Backup_20100216.log

cd j:\

mkdir C_OS

RoboCopy C:\ J:\C_OS /MIR /NP /R:10 /W:10 /XJ /XF BCD.* NTUSER.* USRCLASS.* *.BAK *.tmp /XD $recycle.bin system?volume?information /LOG:d:\Dr_C_OS_Backup_20100216.log

D:

```
Net start OracleServiceIMSProd
Net start OracleServiceIMSDev
Net start OracleServiceIMSTest
Net start OracleServiceTRFProd
Net start OracleServiceTRFDev
Net start OracleServiceTRFTest

Net start OracleServiceTrf09Aug
```

APPENDIX BA. WORKSTATION ACTIVITIES

The work station in F-212B is a Windows XP machine that may no longer be attached to a TFHRC network. This equipment is on the inventory of a FHWA LTPP team member. A replacement will be available at some time in the future.

BACKUPS AND ARCHIVES

Backups of the principal workstation attached to the TFHRC server are intended to have a second on-site copy of scripts, documents and other data related working materials that are used in LTPP database activities. In the event of a computer failure, it is expected that re-establishing the software will be done by the TFHRC Help Desk as is customary for all none COE computers.

A complete copy of the files on the system was made to a 4TB hard drive when the system was taken off the network. Selected files associated with LTPP deliverables were transferred to the new server for archival purposes.

WORKSTATION SOFTWARE

The software on the workstation had all of the appropriate licenses when network access was discontinued in 2013.

The work station software includes the standard distribution from FHWA (Windows XP, MS Office, Winzip, Roxio Creator, Adobe Acrobat 9, and Symantec Endpoint Protection) in addition to LTPP specific items. The LTPP items include Oracle 10g and 11g clients, TextPad, Notepad++. The Oracle software is licensed by FHWA. Notepad++ is freeware.